

⑨대한민국특허청(KR)
⑩공개특허공보(A)

⑪Int. Cl.
H 04 K 1/00

제 2904 호

⑬공개일자 1998. 4. 30

⑪공개번호 98-13071

⑭출원일자 1997. 1. 10

⑭출원번호 97- 412

⑮우선권주장 ⑯1996. 1. 12
1996. 7. 31

⑯96-3997
96-202491

⑰일본(JP)

심사청구 : 있음

⑲ 발 명 자 다케다 노리코

일본국 도쿄도 지요다구 마루노우치 2-2-3 미쓰비시덴키(주)내

시노다 세이이치

일본국 도쿄도 지요다구 마루노우치 2-2-3 미쓰비시덴키(주)내

하세야마 스미오

일본국 도쿄도 지요다구 마루노우치 2-2-3 미쓰비시덴키(주)내

⑳ 출 원 인 미쓰비시덴키(주) 대표자 기타오카 다카시

일본국 도쿄도 지요다구 마루노우치 2-2-3

㉑ 대리인 변리사 백 남 기

(전 59 면)

㉒ 암호화시스템

㉓ 요 약

통신망에 있어서의 암호통신에 관한 것에 관한 것으로서, 암호통신을 실행하는 통신단말과 암호장치를 용이하게 물리적으로 또는 논리적으로 그룹화할 수 있는 암호화시스템을 얻고, 암호장치에 있어서, 암호통신과 평문통신의 전환이 가능한 암호화시스템을 얻기 위해, 암호장치(41), (42)는 섹션키 기억수단(711), (721)에 섹션키를 기억시키고, 섹션키에 의해 통신데이터를 암호화/복호할지 복호하지 않을지를 설정하는 모드스위치(712), (722)를 구비하고, 키관리장치(3)은 섹션키 생성수단(31)이 생성한 그룹마다 개별의 섹션키와 암호장치의 모드스위치(712), (722)의 전환을 유효로 할지 무효로 할지 유효무효 설정수단(61)이 설정한 유효무효정보를 각 암호장치로 배송하고, 암호장치의 유효무효 판정수단(713), (723)은 모드스위치의 설정과 송신된 유효무효 정보로부터 통신데이터를 암호통신으로 할지 평문통신으로 할지를 판정하는 구성으로 하였다.

이러한 구성에 의해, 그룹화된 여러개의 통신단말 사이에서 통신데이터를 암호화 또는 복호화 할 수 있다는 등의 효과가 있다.

※ 대표도 도2

도면의 간단한 설명

도1은 본 발명의 실시형태1에 있어서의 네트워크 시스템을 도시한 도면, 도2는 본 발명의 실시형태1에 있어서의 암호화시스템의 블록도, 도3은 도2에 있어서의 암호화시스템의 섹션키의 배송수순을 도시한 시퀀스도.

도4는 도2에 있어서의 암호화시스템의 그룹분류를 설명하는 도면, 도5는 암호화시스템에 있어서의 유효무효 정보 설정용 화면의 예를 도시한 도면, 도6은 KEYDIST 커맨드로 설정되는 내용을 도시한 도면, 도7은 도2에 있어서의 유효무효 판정수단의 논리곱의 결과를 설명하는 도면, 도8은 도4에 있어서의 모드스위치의 전환과 유효무효 정보 설정후의 평문통신에서의 통신데이터의 흐름을 도시한 도면, 도9는 도2에 있어서의 암호화시스템의 다른 구성을 도시한 블록도, 도10은 도2에 있어서의 암호화시스템의 다른 구성을 도시한 블록도, 도11은 본 발명의 실시형태2에 있어서의 암호화시스템의 블록도, 도12는 도11에 있어서의 암호화시스템의 네트워크예를 도시한 도면, 도13는 도11에 있어서의 암호화시스템의 네트워크예를 도시한 도면, 도14는 도11에 있어서의 암호화시스템의 네트워크예를 도시한 도면, 도15는 도11에 있어서의 암호화시스템의 네트워크예를 도시한 도면, 도16는 도11에 있어서의 암호화시스템의 논리그룹을 설명하기 위한 도면, 도17은 도11에 있어서의 암호화시스템의 다른 구성예를 도시한 블록도, 도18은 도11에 있어서의 암호화시스템의 다른 구성예를 도시한 블록도, 도19는 본 발명의 실시형태3에 있어서의 네트워크 시스템을 도시한 도면, 도20은 NODE형 암호장치를 도시한 도면, 도21은 HUB형 암호장치를 도시한 도면, 도22는 본 발명의 실시형태3에 있어서의 암호화시스템의 블록도, 도23은 도22에 있어서의 암호화조건 기억수단에 기억시키는 암호화조건의 예를 도시한 도면, 도24는 도22에 있어서의 포트조건 기억수단에 기억시키는 포트조건의 예를 도시한 도면, 도25는 도24에 도시한 포트조건에 있어서의 기본패스와 특예패스의 관계를 설명하는 도면, 도26은 도19에 도시한 네트워크 시스템에 있어서 형성되는 새로운 그룹을 도시한 도면, 도27은 HUB형 암호장치를 사용한 통신형태의 예를 도시한 도면, 도28은 도27에 있어서의 통신단말(22)의 포트조건의 설정을 설명하는 도면, 도29는 LAN에 접속하는 암호장치의 도면, 도30은 LAN에 접속하는 암호장치의 제1설치예를 도시한 도면, 도31은 LAN에 접속하는 암호장치의 제2설치예를 도시한 도면, 도32는 LAN에 접속하는 암호장치를 사용한 통신형태를 도시한 도면, 도33은 도32에 도시한 암호장치(503)에 있어서의 암호조건을 설명하는 도면, 도34는 본 발명의 실시형태4에 있어서의 네트워크 시스템을 도시한 도면, 도35는 본 발명의 1실시형태에 있어서의 관리장치(503)의 블록도, 도36은 도35에 도시한 섹션키 테이블을 도시한 도면, 도37은 도34에 도시한 네트워크 시스템에 있어서 암호관리 도메인을 초과한 그룹의 예를 도시한 도면, 도38은 종래의 암호통신 시스템을 도시한 구성도, 도39는 도38에 있어서의 섹션키 문의수단의 상세한 구성을 도시한 구성도, 도40은 종래의 암호통신 시스템에 있어서의 섹션키의 배송순서를 도시한 시퀀스도.

<도면의 주요 부분에 대한 부호의 설명>

1 : LAN, 3, 3a, 6, 6a, 7, 71, 72, 73 : 관리장치, 5 : 입출력장치, 12 : 라우터/브리지, 13 : 네트워크 관리장치, 14, 141~146 : 라우터, 15 : LAN / WAN, 16 : 인터넷, 17 : WAN 20~29, 2a~2m : 통신단말, 31 : 섹션키 생성수단, 32 : 섹션키 관리수단, 33 : 섹션키 송신개시 검출수단, 34 : 섹션키 암호화수단, 35 : 섹션키 송신수단, 37 : 통신장치 그룹 기억수단, 41, 41a, 41b, 42a, 42b, 43~46, 49, 51~54, 81, 81a, 81b, 82, 82a, 82b, 83~88, 501~503 : 암호장치, 61 : 유효무효 설정수단, 62 : 암호화조건 설정수단, 63 : 포트조건 설정수단, 64 : 섹션키 테이블, 65 : 섹션키 수신수단, 66 : 섹션키 복호수단, 91 : 서버, 92 : WWW 대리서버, 93 : WWW, 94 : 메일 서버, 95, 903 : WWW 서버, 96 : 메일서버 A, 97, 98 : 사내메일서버, 99 : 인사파일서버, 121, 122 : 일반 HUB, 131, 132 : 이서넷 스위치, 151 : 브리지, 211, 221 : 어플리케이션, 212, 222 : 통신제어수단, 411, 421 : 섹션키 복호수단, 412, 422 : 섹션키 수신수단, 413, 423 : 암호처리수단, 414, 424 : 데이터 송수신수단, 711, 721 : 섹션키 기억수단, 712, 722 : 모드스위치, 713, 723 : 유효무효 판정수단, 811, 821 : 암호화조건 기억수단, 812, 822 : 조건판정수단, 901 : EOA 서버, 902 : 뉴스버서, 902, 905 : DB 서버.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 통신망에 있어서의 암호통신에 관한 것이다.

종래의 암호통신시스템으로서 예를 들면 사단법인 전자정보 통신학회 발행의 신학기보 OFS-38(1994-3) P. 7~P.12 「LAN 암호통신방식의 실장과 평가」에 기재된 바와 같은 통신단말 및 키관리 워크스테이션내에 암호통신보드를 배치하고, 로컬에리어 네트워크(이하, LAN이라 한다)에 접속하는 구성의 시스템이 있다.

도38은 이와 같은 종래의 암호통신시스템을 도시한 구성도이다.

도면에 있어서, (10)은 LAN, (210), (220)은 이 LAN(10)에 암호장치(410), (420)을 거쳐서 접속된 통신단말, (30)은 키관리장치이다. 또한, 도시하고 있지 않지만, 통상적으로 더 많은 통신단말 및 암호장치가 접속되어 있다.

통신단말(210), (220)은 각각 어플리케이션(2110), (2210), 통신제어수단(2120), (2220), 암호통신 제어수단(2130), (2230)에 의해 구성된다. 키관리 장치(30)은 섹션키 생성수단(310), 섹션키 관리수단(320), 섹션키 암호화수단(340), 섹션키 송신수단(350), 섹션키 문의수신수단(360)에 의해 구성된다. 또, 암호장치(410), (420)은 각각 섹션키 복호수단(4110), (4210), 사용자데이터 암호화/복호수단(4130), (4230), 사용자데이터 송수신수단(4140), (4240), 섹션키 문의수단(4160), (4260)에 의해 구성된다.

또, 도39는 상기 섹션키 문의수단(4160)의 상세를 도시한 구성도이다. (4161)은 섹션키 기억수단, (4162)는 섹션키 문의 송신수단, (4163)은 섹션키 수신수단이다. 또한, 섹션키 문의수단(4260)도 마찬가지로 구성이다.

다음에, 이와 같은 종래의 암호통신시스템에 있어서의 데이터통신의 수순에 대해 설명한다.

암호를 사용해서 단말 사이에서 통신을 실행하기 위해서는 통신하는 단말에 접속되어 있는 암호장치끼리가 공통의 섹션키를 갖고, 그 섹션키에 의해서 데이터의 암호화/복호를 실행한다. 통신하는 단말에 접속되어 있는 암호장치끼리가 공통의 섹션키를 갖기 위한 수순을 키배송이라 한다.

암호통신을 실행할 때에는 키배송의 수순과 실제의 사용자데이터의 송수신 수순이 필요하다. 종래의 암호통신시스템에 있어서는 임의의 통신상대와의 실제의 사용자데이터의 송수신 수순을 실행할 때에는 그 수순을 실행할 때마다 이것에 앞서 키배송의 수순을 실행하는 것이었다.

여기서는 통신단말(210)의 어플리케이션(2110)이 LAN(10)을 거쳐서 접속되어 있는 통신단말(220)의 어플리케이션(2210)과 통신을 실행할 때의 키배송 수순에 대해 설명한다.

이하의 설명에 있어서 처음에 통신을 실행하고자 하는 통신단말(210)의 어드레스를 A로 한다. 또, 통신단말(220)의 어드레스를 B로 한다.

도40은 종래의 암호통신시스템에 있어서의 섹션키의 배송수순을 도시한 시퀀스도이다.

통신단말(210)의 어플리케이션(2110)이 LAN(10)을 거쳐서 접속되어 있는 통신단말(220)의 어플리케이션(2210)과 통신을 실행할 때에는 우선 어플리케이션(2110)이 통신제어수단(2120)을 기동한다. 그리고, 통신상대의 단말인 통신단말(220)의 어드레스B의 정보를 통신제어수단(2120)에 전달한다.

통신제어수단(2120)은 통신단말(220)의 어드레스B를 기억장치(도시하지 않음)에 기억시킴과 동시에 통신단말(220)의 어드레스B의 정보를 암호통신 제어수단(2130)에 전달한다.

암호통신 제어수단(2130)은 어드레스B의 정보를 포함하는 통신개시 요구커맨드를 암호장치(410)으로 보낸다. 통신개시 요구 커맨드는 암호장치(410)의 섹션키 문의수단(4160)의 섹션키 문의 송신수단(4162)로 전달

된다.

섹션키 문의 송신수단(4162)은 상기 통신개시 요구 커맨드에 포함되는 어드레스B의 정보를 구하고 어드레스B의 정보를 포함하는 키배송커맨드KEYREQ를 생성하고, 이것을 LAN(10)을 거쳐서 키관리장치(30)으로 송신한다(S13). 또, 섹션키 기억수단(4161)은 섹션키 문의 송신수단(4162)로부터의 어드레스B의 정보를 기억한다.

다음에, 키관리장치(30)에 의해 수신된 키배송커맨드KEYREQ는 섹션키 문의 수신수단(360)에 전달되고, 여기서 키배송 요구 커맨드의 발신원 어드레스인 어드레스A를 구하고, 이것을 키배송 요구원 어드레스로 한다. 또, 키배송커맨드KEYREQ에 포함되는 정보에서 어드레스B를 구하고 이것을 통신원 어드레스로 하고, 이들을 섹션키 관리수단(320)에 전달한다.

섹션키 관리수단(320)은 키배송 요구원 어드레스인 어드레스A와 통신원 어드레스인 어드레스B의 조합을 기억장치(도시하지 않음)에 기억시킴과 동시에 섹션키 생성수단(310)을 기동한다.

섹션키 생성수단(310)은 섹션키 관리수단(320)에 의해 기동되면 난수를 발생하고 이것을 섹션키로서 섹션키 관리수단(320)에 전달한다.

섹션키 관리수단(320)은 이 섹션키를 기억장치에 기억되어 있는 키배송 요구원 어드레스인 어드레스A와 통신원 어드레스인 어드레스B의 조합의 조로서 기억장치에 기억시킴과 동시에 섹션키 암호화수단(340)에 전달한다.

섹션키 암호화수단(340)은 이 섹션키를 미리 설정되어 있는 섹션키를 암호화하는 키인 마스터키(키암호화키)에 의해 암호화하고, 그 결과를 암호화 섹션키로서 섹션키 관리수단(320)에 전달한다.

섹션키 관리수단(320)은 암호화 섹션키와 기억장치에 기억되어 있는 키배송 요구원 어드레스인 어드레스A와 통신원 어드레스인 어드레스B의 조합을 섹션키 송신수단(350)에 전달한다.

섹션키 송신수단(350)은 암호화 섹션키와 통신지 어드레스인 어드레스B의 정보를 포함한 섹션키 배송 커맨드KEYDIST를 생성하고, 이것을 키배송 요구원 어드레스인 어드레스A의 통신단말(210)에 접속되어 있는 암호장치(410)에 대해서 송신한다(S14).

암호장치(410)에 의해 수신된 섹션키 배송 커맨드KEYDIST는 섹션키 문의수단(4160)의 섹션키 수신수단(4163)에 전달된다.

섹션키 수신수단(4163)은 섹션키 배송 커맨드KEYDIST에서 암호화 섹션키와 통신원 어드레스인 어드레스B의 정보를 구하고 통신지 어드레스인 어드레스B를 기억장치에 기억시킴과 동시에 암호화 섹션키를 섹션키 복호수단(4110)에 전달한다.

섹션키 복호수단(4110)은 암호화 섹션키를 미리 설정되어 있는 마스터키에 의해 복호하고 그 결과를 섹션키로서 섹션키 수신수단(4163)에 전달한다.

섹션키 수신수단(4163)은 섹션키를 섹션키 기억수단(4161)에 전달한다. 또, 키관리장치(30)에 대해 섹션키 수신확인 커맨드KEYDIST-ACK를 송신한다(S15). 또, 섹션키 기억수단(4161)은 기억장치에 기억되어 있는 통신지 어드레스인 어드레스B의 정보와 이 섹션키의 조를 기억장치에 기억시킨다.

키관리장치(30)에 의해 수신된 섹션키 수신확인 커맨드KEYDIST-ACK는 섹션키 송신수단(350)에 전달되고, 이 커맨드의 발신원 어드레스인 어드레스A를 구하고 이것을 키배송 요구원 어드레스로 하고, 이것을 기억장치에 기억시킴과 동시에 섹션키 관리수단(320)에 전달한다.

섹션키 관리수단(320)은 이 키배송 요구원 어드레스와 기억장치에 기억되어 있는 키배송 요구원 어드레스를 대조(照合)한다. 일치하는 키배송 요구원 어드레스와의 조로서 기억되어 있는 통신지 어드레스인 어드레스B와 섹션키 중, 통신지 어드레스인 어드레스B를 기억장치에 기억시킴과 동시에 섹션키 암호화수단(340)에 이

섹션키를 전달한다.

섹션키 암호화수단(340)은 이 섹션키를 미리 설정되어 있는 마스터키에 의해 암호화하고, 그 결과를 암호화 섹션키로서 섹션키 관리수단(320)에 전달한다.

섹션키 관리수단(320)은 이 암호화 섹션키와 기억장치에 기억되어 있는 통신지 어드레스인 어드레스B의 조합을 섹션키 송신수단(350)에 전달한다. 섹션키 송신수단(350)은 이 암호화 섹션키와 기억장치에 기억되어 있는 키배송 요구원 어드레스인 어드레스A의 정보를 포함한 섹션키 배송 커맨드KEYDIST를 생성한다. 이것을 통신지 어드레스인 어드레스B의 통신단말에 접속되어 있는 암호장치인 암호장치(420)에 대해서 송신한다(S16).

암호장치(420)에서는 상기 암호장치(410)과 마찬가지로 동작이 실행되고, 키관리장치(30)에 대해 섹션키 수신확인 커맨드KEYDIST-ACK를 송신한다(S17).

키관리장치(30)에 의해 수신된 섹션키 수신확인 커맨드KEYDIST-ACK는 섹션키 송신수단(350)에 전달되고, 이 커맨드의 발신원 어드레스인 어드레스B를 구하여 이것을 통신지 어드레스로 하고, 이것을 기억장치에 기억시킴과 동시에 섹션키 관리수단(320)에 전달한다.

섹션키 관리수단(320)은 이 통신지 어드레스와 기억장치에 기억되어 있는 통신지 어드레스를 대조하고, 일치하는 통신지 어드레스와의 조로서 기억되어 있는 키배송 요구원 어드레스인 어드레스A를 섹션키 송신수단(350)에 전달한다.

섹션키 송신수단(350)은 기억장치에 기억되어 있는 통신지 어드레스인 어드레스B의 정보를 포함한 통신개시 커맨드START를 생성한다. 이것을 키배송 요구원 어드레스인 어드레스A의 통신단말에 접속되어 있는 암호장치(410)에 대해서 송신한다(S18).

암호장치(410)에 의해 수신된 통신개시 커맨드START는 사용자데이터 송수신수단(4140)에 전달된다. 사용자데이터 송수신수단(4140)은 통신개시 커맨드START에서 통신지 어드레스인 어드레스B의 정보를 구하고, 이것을 기억장치에 기억시킨다. 또, 통신단말(210)에 키배송 확인 커맨드를 보낸다.

키배송 확인 커맨드는 통신단말(210)의 암호통신 제어수단(2130)에 전달된다. 암호통신 제어수단(2130)은 이 키배송 확인 커맨드에 포함되는 통신지 어드레스인 어드레스B의 정보를 구해서 이것을 통신상대 어드레스로 하고, 이 통신상대 어드레스와 통신개시 플래그를 온으로 한 정보의 조를 기억장치에 기억시킨다. 또, 통신제어수단(2120)에 이 통신상대 어드레스의 정보를 포함하는 통신개시통지를 전달한다.

이상의 수순에 따라서 키배송이 실행되는 것에 의해 암호장치(410)과 암호장치(420)이 공통의 섹션키를 가질 수 있다.

다음에, 통신단말(210)의 어플리케이션(2110)이 LAN(10)을 거쳐서 접속되어 있는 통신단말(220)의 어플리케이션(2210)과 통신을 실행할 때의 사용자데이터의 전송의 수순에 대해 상세하게 설명한다.

통신단말(210)의 어플리케이션(2110)은 사용자데이터와 통신단말(220)의 어드레스B의 조를 통신제어수단(2120)에 전달한다. 통신제어수단(2120)은 이 사용자데이터와 통신단말(220)의 어드레스B의 조를 암호장치(410)으로 보낸다.

이 사용자데이터와 통신단말(220)의 어드레스B의 조는 사용자데이터 송수신수단(4140)에 전달된다. 사용자데이터 송수신수단(4140)은 이 사용자데이터와 통신단말(220)의 어드레스B의 조를 사용자데이터 암호화/복호수단(4130)에 전달한다.

사용자데이터 암호화/복호수단(4130)은 통신단말(220)의 어드레스B에 의해 기억장치에 기억되어 있는 어드레스와 섹션키의 조를 대조하고, 통신상대 어드레스B와의 조로서 기억되어 있는 섹션키를 사용하여 이 사용

자데이터를 암호화 한다. 이것을 암호화 사용자데이터로 하고, 이 암호화 사용자데이터와 통신상대 어드레스의 조를 사용자데이터 송수신수단(4140)에 전달한다.

사용자데이터 송수신수단(4140)은 이 암호화 사용자데이터와 통신상대 어드레스B의 조에서 암호화 사용자데이터의 정보를 포함하는 사용자데이터 송신 커맨드를 암호장치(420)로 보낸다.

암호장치(420)에 의해 수신된 사용자데이터 송신 커맨드는 사용자데이터 송수신수단(4240)에 전달된다. 사용자데이터 송수신수단(4240)은 이 사용자데이터 송신 커맨드에 포함되는 암호화 사용자데이터 및 통신상대 어드레스A의 정보를 구하고 이 암호화 사용자데이터와 어드레스A의 조를 사용자데이터 암호화/복호수단(4230)에 전달한다.

사용자데이터 암호화/복호수단(4230)은 통신상대 어드레스A에 의해 기억장치에 기억되는 어드레스와 섹션키의 조를 대조하고, 어드레스A와의 조로서 기억되어 있는 섹션키를 사용해서 이 사용자데이터를 복호한다. 이것을 사용자데이터로 하고, 이 사용자데이터와 통신상대 어드레스의 조를 사용자데이터 송수신수단(4240)에 전달한다. 사용자데이터 송수신수단(4240)은 이 사용자데이터와 어드레스의 조를 통신단말(220)에 전달한다. 통신단말(220)에 전달된 이 사용자데이터와 통신상대 어드레스의 조는 통신제어수단(2220)에 전달된다. 통신제어수단(2220)은 이 사용자데이터와 통신상대 어드레스의 조를 어플리케이션(2210)에 전달한다.

이상과 같이 종래의 암호통신 시스템에 있어서는 임의의 통신상대와의 실제의 사용자데이터의 송수신 수순을 실행할 때에는 그 수순을 실행할 때마다 이것에 앞서 키배송 수순을 실행할 필요가 있다. 또, 통신상대마다 암호키의 정보를 등록할 필요가 있다. 또, 암호를 사용하기 때문에 통신단말에 암호통신 제어수단이라고 하는 특별수단을 추가할 필요가 있다.

또, 일본국 특허공개 공보 소화54-93937호에는 여러개의 도메인 데이터통신 네트워크에 있어서의 “암호장치용 공통조작키 설정장치”에 대해서 개시되어 있다.

발명이 이루고자 하는 기술적과제

이상 기술한 바와 같이 종래의 암호데이터통신의 수순에 의하면, 통신단말은 각 통신상대마다 통신을 개시하기 위해 앞서 그 통신에서 사용하는 섹션키를 섹션키 관리장치에 요구하고, 그것에 따라서 키관리장치에서 통신단말로 섹션키를 배송하도록 되어 있었다. 그 때문에, 동일한 부분의 통신단말끼리를 그룹화하는 것에 관해서는 고려되어 있지 않았다.

또, 암호장치에 접속된 통신단말은 전자메일 등의 평문통신(암호화되지 않은 통신)을 송수신할 수 없다는 과제가 있었다.

또, 통신상대로 되는 통신단말, 어플리케이션, 통신방향에 따라 평문통신으로 할지 또는 암호통신으로 할지를 설정하는 불가능하였다. 또, 여러개의 키중에서 임의의 키를 사용해서 암호화한다고 하는 설정도 불가능하였다.

또, 1대의 암호장치에 여러대의 통신단말이 접속되는 경우, 통신단말마다 다른 조건으로 암호화하는 것은 불가능하였다.

또, 일본국 특허공개 공보 소화54-93937호에서는 여러개의 도메인 사이에서 데이터통신을 암호화하기 위한 공통의 암호화키를 설정하는 것이 기술되어 있었지만, 공통의 암호화키를 사용하여 여러개의 중복된 그룹을 실현하는 방식은 기술되어 있지 않았다.

본 발명의 목적은 상기와 같은 과제를 해결하기 위해 이루어진 것으로, 1개의 네트워크상의 암호데이터통신을 실행하는 통신장치에서 여러개의 물리그룹을 형성할 수 있는 암호화시스템을 제공하는 것이다.

또, 본 발명의 다른 목적은 임의의 암호장치에 있어서 암호통신과 평문통신을 전환할 수 있는 암호화시스템을 제공하는 것이다.

또, 본 발명의 또 다른 목적은 동일한 네트워크상 또는 여러개의 도메인 사이에 여러개의 중복된 논리그룹을 실현하는 암호화시스템을 제공하는 것이다.

발명의 구성 및 작용

본 발명에 관한 암호화시스템은 그룹화된 여러개의 통신장치 및 적어도 상기 여러개의 통신장치의 1개 이상의 통신장치에 대응해서 각각 마련된 여러개의 암호장치로서, 상기 그룹에 속하는 통신장치가 송수신하는 통신데이터를 암호화 또는 복호하는 섹션키를 적어도 1개 기억하는 섹션키 기억수단, 상기 섹션키에 의해 통신데이터를 암호화 또는 복호하는 암호처리수단 및 상기 암호처리수단에 의해 처리된 통신데이터를 송수신하는 데이터 송수신수단을 구비한 여러개의 암호장치를 구비한 것을 특징으로 한다.

상기 암호장치는 상기 섹션키 기억수단에 섹션키를 적어도 1개 기억시키고, 상기 섹션키에 의해 통신데이터를 암호화 또는 복호할지 하지 않을지를 설정하는 모드스위치를 구비하는 것을 특징으로 한다.

상기 암호장치는 또, 통신데이터의 암호화에 관한 암호화조건을 기억하는 암호화조건 기억수단 및 상기 암호화조건에 따라서 통신데이터를 암호화 또는 복호할지 하지 않을지를 판정하는 조건판정수단을 구비하는 것을 특징으로 한다.

상기 암호화시스템은 또 그룹화된 통신장치를 기억하는 통신장치 그룹 기억수단 및 상기 통신장치그룹 기억수단에 의해 기억된 그룹마다 개별의 섹션키를 생성해서 출력하는 섹션키 생성수단을 구비한 키관리장치를 구비하는 것을 특징으로 한다.

상기 키관리장치는 또 상기 암호장치에 구비된 상기 모드스위치의 전환을 유효로 할지 무효로 할지를 나타내는 유효무효정보를 암호장치마다 설정하고 유효무효정보를 대응하는 암호장치로 송신하는 유효무효 설정수단을 구비하고, 상기 암호장치는 또 상기 모드스위치의 설정과 송신된 상기 유효무효정보에서 통신데이터를 암호화 또는 복호할지를 판정하는 유효무효 판정수단을 구비하는 것을 특징으로 한다.

본 발명에 관한 암호화시스템은 여러개의 키관리장치를 구비하고, 각 키관리장치와 1이상의 암호장치와 1이상의 통신장치로 이루어지는 암호관리도메인을 형성하는 암호화시스템에 있어서, 상기 여러개의 키관리장치는 각각의 암호관리도메인에서 사용하는 섹션키를 생성하는 섹션키 생성수단을 구비하고, 상기 여러개의 키관리장치중의 1대의 키관리장치에 있어서의 섹션키 생성수단은 또 여러개의 암호관리도메인끼리의 암호통신에 있어서 사용되는 공통 섹션키를 다른 키관리장치를 위해 생성하는 것을 특징으로 한다.

[발명의 실시형태]

실시형태1

이 실시형태에서는 각 암호장치에 섹션키를 1개 기억시키고, 암호통신과 평문통신(암호화하지 않은 통신)을 전환할 수 있는 암호화시스템에 대해서 기술한다.

도1은 이 실시형태에 있어서의 네트워크시스템의 1예를 도시한 도면이다.

2개의 LAN(Local Area Network)이 라우터/브리지(12)에 의해 LAN/WAN(Wide Area Network)(15)와 접속되어 있는 네트워크시스템이다. LAN1에는 키관리장치(3)이 암호장치(49)를 거쳐서 접속된다. 또, LAN1에는 암호장치(41), (42), (43)을 거쳐서 통신단말(통신장치라고도 한다)(21), (22), (23)이 접속된다. 또, 암호장치를 거치지 않는 통신단말(24), (25)가 접속된다. 또, 네트워크 관리장치(13)이 접속된다.

도면에서는 키관리장치(3)에 암호장치(49)가 접속되어 있지만, 이것은 키관리장치(3)이 다른 통신단말과

함께 그룹을 구성하는 경우를 상정하고 있다. 그 때문에, 키관리장치(3)에 암호장치(49)가 접속되어 있지 않아도 좋다. 또, 1대의 암호장치에 대해 여러개의 통신단말을 접속해도 좋다.

암호장치(41)~(43)은 LAN1과 통신단말(21)~(23) 사이에 배치되고, 통신데이터의 데이터부를 암호화/복호하는 것에 의해 LAN1상을 흐르는 통신데이터의 도청을 방지한다. 사용자데이터의 암호화는 고속이고 비역성(秘匿性)이 높은 독자적인 비밀키 암호방식에 의한다. 암호범위는 암호장치를 나와 네트워크상을 통과해서 통신지의 암호장치로 들어갈 때까지이다.

키관리장치(3)은 암호장치에 대한 데이터를 암호화하는 섹션키를 배송함과 동시에 암호장치(41)~(43)의 상태를 상시 감시한다.

도2는 이 실시형태에 있어서의 암호화시스템의 블록도이다.

도2에 있어서, LAN1에 키관리장치(3)과 암호장치(41), (42), ...이 접속되어 있다. 키관리장치(3)에는 입출력장치(5)가 접속된다. 암호장치(41), (42), ...에는 통신단말(21), (22), ...이 접속된다. 도면에는 암호장치(41), (42) 및 통신단말(21), (22)가 도시되어 있지만, 통상적으로 더 많은 암호장치 및 통신단말이 접속된다. 또, 설명을 간단하게 하기 위해 키관리장치(3)에는 암호장치가 접속되지 않은 예를 도시하고 있다. 또, 1대의 암호장치에 대해 1대의 통신단말이 접속되는 예를 도시하고 있다.

통신단말(21), (22)는 각각 어플리케이션(211), (221), 통신제어수단(212), (222)로 구성된다.

키관리장치(3)은 섹션키 생성수단(31), 섹션키 관리수단(31), 섹션키 관리수단(32), 섹션키 송신개시 검출수단(33), 섹션키 암호화수단(34), 섹션키 송신수단(35), 통신장치 그룹 기억수단(37), 유효무효 설정수단(61)로 이루어진다. 섹션키 생성수단(31)은 데이터를 암호화하는 섹션키를 생성한다. 섹션키 암호화수단(34)는 섹션키 생성수단(31)에 의해 생성된 섹션키를 키암호화키를 사용해서 또 암호화한다.

섹션키 송신수단(35)는 섹션키를 각 암호장치로 송신한다. 통신장치 그룹 기억수단(37)은 그룹화된 통신장치를 기억한다. 유효무효 설정수단(61)은 암호장치에 구비된 모드스위치의 전환을 유효로 할지 무효로 할지를 나타내는 유효무효정보를 암호장치마다 설정한다. 그리고, 설정한 유효무효정보를 대응하는 암호장치로 송신한다.

암호장치(41), (42)는 섹션키 복호수단(411), (421), 섹션키 수신수단(412), (422), 암호처리수단(413), (423), 데이터 송수신수단(414), (424), 섹션키 기억수단(711), (721), 모드스위치(712), (722), 유효무효 판정수단(713), (723)으로 이루어진다. 섹션키 수신수단(412), (422)는 키관리장치(3)에서 송신된 암호화된 섹션키를 수신한다. 섹션키 복호수단(411), (421)은 섹션키 수신수단(412), (422)에 의해 수신되고 암호화된 섹션키를 각각의 암호장치의 독자적인 키암호화키에 의해 복호한다. 암호처리수단(413), (423)은 섹션키에 의해 통신데이터를 암호화 또는 복호한다. 데이터 송수신수단(414), (424)는 암호처리수단(413), (423)에 의해 처리된 통신데이터를 송수신한다. 섹션키 기억수단(711), (721)은 통신데이터를 암호화 또는 복호하는 섹션키를 적어도 1개 기억한다. 모드스위치(712), (722)는 이 암호장치에 있어서의 통신데이터를 암호 통신으로 할지 평문통신으로 할지를 설정하는 스위치이다. 유효무효 판정수단(713), (723)은 암호장치에 있어서의 모드스위치(712), (722)의 설정과 키관리장치(3)에서 송신된 유효무효정보에서 통신데이터를 암호통신으로 할지 평문으로 할지를 판정한다.

섹션키와 키암호화키에 대해서 기술한다.

섹션키는 사용자데이터를 암호화하는 키이다. 이것에 반해 키암호화키는 섹션키를 암호화하는 키이다. 키암호화키는 키관리장치(3)에서 각 암호장치로 섹션키를 배송할 때 제3자에게 섹션키를 알리지 않고 배송하기 위해 사용한다. 키관리장치(3)의 섹션키 암호화수단(34)에서 섹션키를 키암호화키에 의해 암호화한다. 암호장치(41), (42)의 섹션키 복호수단(411), (421)에 의해 배송되어 암호화된 섹션키를 키암호화키에 의해 복호한다.

키암호화키는 암호장치마다 다르다.

키암호화키의 설정방법은 통신회선을 거치지 않는다.

다음에, 키암호화키의 설정수순을 기술한다.

1. 키관리장치(3)에서 각 암호장치마다 다른 키암호화키를 작성한다.
2. 암호장치에 접속된 로컬/몬솔에서 키암호화키를 설정하는 커맨드를 입력하고 키입력모드로 한다.
3. 키관리장치에서 작성한 키암호화키를 암호장치의 로컬/몬솔에서 입력한다.
4. 암호장치를 재차 들어올린다.

섹션키는 사용자데이터를 암호화/복호하기 위해 사용된다. 동일 그룹의 암호장치의 섹션키는 완전히 동일하다. 단, 후술의 실시형태에서 기술하는 바와 같이 섹션키를 여러개 준비하면, 암호장치 사이에서 중복된 논리그룹을 형성하는 것이 가능하다.

섹션키의 설정방법은 온라인에 의해 설정한다.

다음에, 섹션키를 암호장치의 요구에 따라 설정하는 수순의 개략을 기술한다.

1. 키관리장치(3)에서 섹션키를 작성한다.
2. 작성된 섹션키를 각 암호화장치마다 다른 키암호화키에 의해 암호화한다.
3. 암호장치의 전원을 넣는 것에 의해 자동적으로 암호장치에서 섹션키를 송신해 받도록 요구커맨드가 키관리장치(3)으로 보내진다.
4. 키관리장치(3)에서 암호화된 섹션키가 요구가 있었던 암호장치로 보내진다.

다음에, 다른 방법으로서 섹션키를 관리자의 지시에 따라 설정하는 수순의 개략을 기술한다.

1. 키관리장치(3)에서 섹션키를 작성한다.
2. 작성된 섹션키를 각 암호화장치마다 다른 키암호화키에 의해 암호화한다.
3. 관리자의 지시에 따라 새로운 섹션키를 송신하는 암호장치의 범위를 결정한다. 범위의 종류는 크게 나누어 다음의 4종류가 있다.

- [1] 직전의 암호장치의 상태확인시에 전원이 온이었던 암호장치 전체.
- [2] 직전의 암호장치의 상태확인시에 전원이 온이고 또한 미리 지정된 그룹내의 암호장치 전체.
- [3] 지정된 암호장치.
- [4] 모든 암호장치.
4. 결정된 범위에 포함되는 암호장치 전체로 암호화된 섹션키를 배송한다.

다음에, 다른 방법으로서 키관리장치(3)에 타이머를 구비하고, 일정시간이 경과하면 자동적으로 섹션키를 생성하고 동일 그룹에 속하는 암호장치로 배송하는 수순을 도2를 사용해서 상세하게 기술한다.

LAN1에 접속되고 동일 그룹에 속하는 각 암호장치에 대해 일정시간마다 섹션키를 키관리장치(3)에서 배포하고, 그때까지 설정되어 있던 섹션키를 즉시 배포된 섹션키에 의해 치환하는 예이다.

통신단말(21)과 통신단말(22), 즉 암호장치(41), (42)가 그룹1로서 그룹화되고, 통신장치 그룹 기억수단(37)에 등록되어 있다.

암호통신을 실행할 때에는 키배송 수순과 실제의 사용자데이터의 송수신 수순이 필요하지만, 키배송 수순과 실제의 사용자데이터의 송수신 수순은 독립적으로 실행하는 것이 특징이다.

도3은 섹션키의 배송 수순을 도시한 시퀀스도이다.

S1은 섹션키 배송 커맨드KEYDIST, S2는 섹션키 수신확인 커맨드KEYDIST-ACK, S3은 섹션키 배송 커맨드KEYDIST, S4는 섹션키 수신확인 커맨드KEYDIST-ACK이다.

(수순1-1) 키관리장치(3)의 섹션키 송신개시 검출수단(33)의 그룹1대응의 타이머가 타이머아웃되면, 섹션키 송신개시 검출신호를 섹션키 관리수단(32)에 전달한다.

(수순1-2) 섹션키 관리수단(32)은 이 섹션키 송신개시 검출신호를 수취하면, 섹션키 생성수단(31)을 기동한다.

(수순1-3) 섹션키 생성수단(31)은 섹션키 관리수단(32)에 의해 기동되면 난수를 발생하고 이것을 섹션키로서 섹션키 관리수단(32)에 전달한다.

(수순1-4) 섹션키 관리수단(32)은 이 섹션키를 그룹1의 섹션키로서 기억장치에 기억시킨다. 섹션키 관리수단(32)은 통신장치그룹 기억장치(37)에서 그룹1에 속하는 암호장치를 검색하고, 암호장치(41)을 선택한다. 섹션키 관리수단(32)은 섹션키 암호화수단(34)에 이 섹션키를 전달하고, 암호장치(41)에 대한 키암호화인 사실을 알린다.

(수순1-5) 섹션키 암호화수단(34)은 이 섹션키를 암호장치(41)에 대응하는 키암호화키에 의해 암호화하고 그 결과를 암호화 섹션키로서 섹션키 관리수단(32)에 전달한다.

(수순1-6) 섹션키 관리수단(32)은 이 암호화 섹션키와 암호장치(41)의 어드레스를 섹션키 송신수단(35)에 전달한다.

(수순1-7) 섹션키 송신수단(35)은 이 암호화 섹션키의 정보를 포함한 섹션키 배송 커맨드KEYDIST를 생성하고, 이것을 기억장치에 기억시킨다. 섹션키 송신수단(35)은 이 섹션키 배송 커맨드KEYDIST를 전달된 어드레스에 의해 암호장치(41)에 대해서 송신한다(S1).

(수순1-8) 암호장치(41)의 섹션키 수신수단(412)에 의해 이 섹션키 배송 커맨드KEYDIST는 수신된다.

(수순1-9) 섹션키 수신수단(412)은 이 섹션키 배송 커맨드KEYDIST에서 암호화 섹션키를 포함하는 데이터 부분을 추출하고 섹션키 복호수단(411)에 전달한다.

(수순1-10) 섹션키 복호수단(411)은 이 암호화 섹션키를 포함하는 데이터 부분을 미리 다른 수단에 의해 설정되어 있는 암호장치(41)의 독자적인 키암호화키에 의해 복호한다. 그리고, 그 결과를 섹션키로서 섹션키 수신수단(412)에 전달한다.

(수순1-11) 섹션키 수신수단(412)은 키관리장치(3)에 대해 섹션키 수신확인 커맨드KEYDIST-ACK를 송신한다(S2). 또, 이 섹션키를 섹션키 기억수단(711)에 기억시킨다.

(수순1-12) 키관리장치(3)에 의해 수신된 암호장치(41)로부터 섹션키 수신확인 커맨드KEYDIST-ACK는 섹션키 송신수단(35)에 전달된다. 섹션키 송신수단(35)은 섹션키 관리수단(32)에 대해 암호장치(41)로 섹션키 배송 완료통지를 통지한다. 섹션키 관리수단(32)은 섹션키 암호화수단(34)에 그룹1의 섹션키를 전달하고, 암호장치(42)에 대한 암호화인 사실을 알린다.

(수순1-13) 섹션키 암호화수단(34)은 상기 (수순1-5)와 마찬가지로 해서 암호장치(42)에 대응하는 암호화 섹션키를 작성한다. 섹션키 송신수단(35)은 이 암호화 섹션키의 정보를 포함한 섹션키 배송 커맨드KEYDIST를 작성하고, 암호장치(42)로 송신한다(S3).

(수순1-14) 암호장치(42)의 섹션키 수신수단(422)에 의해 이 섹션키 배송 커맨드는 수신된다.

(수순1-15) 섹션키 수신수단(422)은 이 섹션키 배송 커맨드에서 암호화 섹션키를 추출하고, 이 암호화 섹션키를 섹션키 복호수단(421)에 전달한다.

(수순1-16) 섹션키 복호수단(421)은 이 암호화 섹션키를 미리 다른 수단에 의해 설정되어 있는 독자적인 키암호화키에 의해 복호한다. 그 결과를 섹션키로서 해서 섹션키 수신수단(422)에 전달한다.

(수순1-17) 섹션키 수신수단(422)은 키관리장치(3)에 대해 섹션키 수신확인 커맨드KEYDIST-ACK를 송신한다

다(S4). 또, 이 섹션키를 섹션키 기억수단(721)에 기억시킨다.

(수순1-18) 키관리장치(3)에 의해 수신된 섹션키 수신확인 커맨드KEYDIST-ACK는 섹션키 송신수단(35)에 전달된다.

(수순1-19) 섹션키 송신수단(35)는 암호장치(42)로의 섹션키 배송완료를 섹션키 관리수단(32)에 통지한다. 섹션키 관리수단(32)는 그룹1에 속하는 다른 암호장치가 없으므로 그룹1에 대한 키배송은 완료되었다고 판단한다.

이상의 수순에 따라서 키배송이 실행되는 것에 의해 동일 그룹에 속하는 암호장치(41)와 암호장치(42)가 공통의 섹션키를 가질 수 있다.

그 후, 통신단말(21)의 어플리케이션(211)이 LAN1을 거쳐서 접속되어 있는 통신단말(22)의 어플리케이션(221)과 통신을 실행한다. 어플리케이션(211)의 사용자데이터는 암호장치(41)의 암호처리수단(413)에 의해 암호화되고 암호장치(42)의 암호처리수단(423)에 의해 복호되며 어플리케이션(221)에 전달된다.

또, 상기의 섹션키 송신개시 검출수단(33)에 있어서의 섹션키 송신개시 검출신호를 타이머에 관계없이 키관리장치(3)의 관리자에 의한 수동의 입력조작에 의해 출력하도록 해도 좋다.

또, 상기의 섹션키 송신개시 검출수단(33)에 있어서의 섹션키 송신개시 검출신호를 암호장치의 들어올림상태를 검출하는 것에 의해 출력하도록 해도 좋다.

또한, 상기 2대의 암호장치로 키배송을 실행하는 수순을 도시했지만, 동일 그룹에 속하는 임의의 대수의 암호장치에 대해서도 마찬가지로 실행할 수 있다.

섹션키의 변경을 섹션키의 배송/수신과 동시에 실행하는 예를 설명하였다. 그러나, 통신을 한번 정지하고 나서 섹션키를 새로운 키로 변경해도 좋고, 섹션키의 배송/수신부터 소정시간 경과후에 변경해도 좋다.

다음에, 본 실시형태의 요점인 암호통신과 평문통신의 전환에 대해서 기술한다.

도4는 암호화시스템에 있어서의 그룹분류를 설명하기 위한 도면이다.

키관리장치(3)는 암호장치(49)를 거쳐 LAN1에 접속된다. 통신단말(20)~(22), (22)~(29)는 암호장치(41)~(46)을 거쳐 LAN1에 접속된다. 통신단말(21)과 (22)는 동일한 암호장치(42)에 접속된다. 통신단말(28)과 (29)는 동일한 암호장치(46)에 접속된다. 또, 통신장치(23), (24)가 암호장치를 거치지 않고 LAN1에 접속되어 있다.

키관리장치(3)와 암호장치(49)는 그룹A로 한다. 암호장치(41)~(43)과 통신단말(20)~(22), (25)는 그룹B로 한다. 암호장치(44)~(46)과 통신단말(26)~(29)는 그룹C로 한다. 여기서, 예를 들면 통신단말(20)에서 송신된 사용자데이터는 암호장치(41)에서 암호화된다. 암호화된 데이터를 수신할 수 있는 가능성이 있는 통신단말은 통신단말(21), (22), (25)이다. 암호장치를 거치지 않는 통신단말(23), (24)와 그룹C에 속하는 통신단말(26)~(29)는 통신데이터를 복호할 수 없으므로 수신할 수 없다.

이와 같이 암호통신에 있어서 동일 암호그룹의 암호장치에 접속되어 있는 통신단말 사이는 마치 평문통신과 같이 통신할 수 있다. 그러나, 암호그룹이 다른 또는 암호장치가 접속되어 있지 않는 통신단말에서는 암호화된 통신문을 수신해도 복호할 수 없으므로 도청할 수 없다. 만약, 암호장치 그 자체를 도난당해도 어느 암호그룹에 속하고 있는지는 암호장치측에서 분간할 수 없으므로 은연중(なりすまし)에 방지할 수 있다.

그런데, 암호그룹이 다른 또는 암호장치가 접속되어 있지 않는 통신단말과 통신하고자 하는 경우에는 암호장치에서 출입하는 통신을 암호화/복호하는 것을 멈추지 않으면 안된다. 이 전환을 암호장치(41), (42), ...가 갖고 있는 모드스위치(712), (722), ...의 온/오프에 의해 실현한다. 모드스위치(712), (722), ...을 온하면 평문통신으로 되고, 오프로 하면 암호통신으로 된다. 그러나, 암호장치는 통신단말 이용자가 멋대로 조작할 수 있으므로, 모드스위치의 온/오프만으로 암호통신을 평문통신으로 변경할 수 있는 것은 안전상 바람직하지 않다.

그래서, 키관리장치에 의해 모드스위치의 전환을 유효로 할지 무효로 할지 암호장치마다 유효무효정보를 설정한다. 이것에 의해 키관리장치에서 평문통신과 암호통신의 전환이 가능한 암호장치를 관리할 수 있다.

도5는 키관리장치(3)에 의해 설정된 유효무효정보와 유효무효정보를 입력하는 화면이다.

새로 데이터를 입력하는 경우에는 입력필드에서 입력한다. 입력필드에서 입력하는 데이터로서 그룹번호(GN), IP어드레스, 비고, 유효/무효정보가 있다. 화면에 표시되는 그룹명칭은 그룹번호(GN)이 입력되면 자동적으로 화면에 출력된다. 유효무효정보는 미리 '0' (무효)이 설정되어 있다. 유효로 하고자 하는 경우에는 '1' 을 입력한다. 표시되어 있는 데이터는 위부터 순서대로 도4에 도시한 암호장치(49), (41)~(46)에 대응한다. 암호장치(41)과 (46)의 유효무효정보가 유효로 되어 있다. 여기서, 유효라고 하는 것은 이 암호장치의 모드스위치의 전환이 유효라는 의미이다. 무효라도 하는 것은 암호장치에 의해 모드스위치가 전환되어도 무효로 한다는 의미한다.

키관리장치(3)이 암호화된 섹션키를 각 신호장치로 KEYDIST 커맨드에 의해 배송할 때 유효무효정보도 부가해서 보낸다.

도6에 KEYDIST 커맨드의 내용을 도시한다.

도6에 있어서 프로토콜 타입은 통신프로토콜 타입을 나타낸다. 인증용 데이터는 배송된 암호장치에 의해 복호할 수 있었는지 아닌지를 체크하기 위한 고정패턴이다. 암호장치에 의해 복호된 데이터가 일부가 고정패턴과 일치하면 복호가 정확하게 실행된 것을 나타낸다. 최후 비트에 유효무효정보가 설정된다. '1' 은 유효를 나타내고, '0' 은 무효를 나타낸다.

이상과 같이 KEYDIST 커맨드의 내용중 데이터가 설정되지 않는 부분을 0으로 한다. 그리고, 섹션키 및 유효무효정보 등이 설정된 KEYDIST 커맨드의 내용은 키암호화키에 의해 암호화되고 송신된다.

키관리장치(3)에 있어서의 유효무효 설정수단(61)은 입력화면에 의해 설정된 유효무효정보를 섹션키 배송 커맨드 KEYDIST를 생성하는 섹션키 송신수단(35)에 전달한다. 섹션키 송신수단(35)는 도6에 도시한 바와 같이 최후 비트에 유효무효정보를 설정한 KEYDIST 커맨드를 생성한다.

다음에, 암호장치(41)을 예로 들면, 섹션키 수신수단(412)가 KEYDIST 커맨드를 수신하고, 섹션키 복호수단(411)에 전달한다. 섹션키 복호수단(411)이 복호하고, 복호된 섹션키를 섹션키 수신수단(412)에 전달한다. 섹션키 수신수단(412)는 복호된 KEYDIST의 내용에서 유효무효정보를 빼내고 유효무효 판정수단(713)에 전달한다. 유효무효 판정수단(713)은 모드스위치(712)의 스위치의 온/오프와 유효무효정보의 논리곱에 의해서 암호통신으로 할지 평문통신으로 할지를 판정한다.

도7에 모드스위치의 정보와 유효무효정보의 논리곱을 표로서 도시한다.

모드스위치의 오프는 (0)이고, 온은 (1)이다. 유효무효정보가 유효는 (1)이고, 무효는 (0)이다. 그 때문에 논리곱을 취하면 모드스위치가 온이고, 또한 유효무효정보가 유효인 경우에만 (1), 즉 사용자데이터는 무효로 된다. 그 이외의 경우는 모든 모드스위치의 설정여하에 관계없이 암호화된. 또한, 무효라고 하는 것은 평문통신으로 하는 것이다.

도8은 도4와 같이 그룹화된 암호화시스템에 있어서 평문통신을 채용하는 경우이다.

암호장치(41), (43), (44), (46)의 모드스위치가 온으로 되어 있다. 즉, 이들 암호장치는 평문통신으로 하도록 모드스위치가 전환되어 있다. 그런데, 키관리장치(3)의 유효무효정보는 도5에 도시한 바와 같이 암호장치(41)과 (46)만이 유효로 되어 있다. 그 때문에, 통신단말(20)에서 보내진 사용자데이터는 암호장치(41)에서는 암호화되지 않고, 평문으로 송신된다. 평문통신이므로 암호장치가 없는 통신단말(23), (24)에서 수취할 수 있다. 또, 암호장치(46)의 모드스위치가 온이고, 유효무효정보가 유효이므로 통신단말(20)으로부터의 통신데이터를 복호

하지 않는다. 그 때문에 통신단말(28), (29)는 통신단말(20)이 송출한 평문통신을 취할 수 있다. 암호장치(43), (44)는 모드스위치가 온이긴 하지만, 유효무효정보가 무효로 되어 있으므로 평문통신을 수취할 수 없다.

또, 암호장치(41)은 그룹B에 속하지만, 암호장치(46)은 그룹C에 속한다. 평문통신으로 하는 것에 의해 암호장치가 없는 통신단말 또는 다른 그룹의 통신단말과도 통신할 수 있다.

이상과 같이 이 실시형태의 암호화시스템은 암호장치의 섹션키를 그룹단위로 동일한 것으로 하는 것에 의해 다른 그룹간의 통신을 금지할 수 있다. 또, 네트워크상에서의 도청을 방지할 수 있다. 또, 암호통신으로 할지 평문통신으로 할지를 암호장치측 및 관리장치의 설정에 의해 선택할 수 있고, 다른 그룹의 통신단말 또는 암호장치를 갖지 않는 통신단말과 통신할 수도 있어 보다 유연한 암호화시스템을 형성할 수 있다. 또, 암호장치의 모드스위치에 의해 암호통신으로 할지 평문통신으로 할지를 설정하고, 이에 부가해서 관리장치에서 암호장치의 모드스위치가 유효인지 무효인지를 일괄 관리할 수 있으므로 보다 확실한 안전관리를 실행할 수 있다.

또, 도2의 암호장치의 블록도에 있어서, 암호장치(41), (42)의 모드스위치(712), (722)를 제거해도 좋다. 이 경우, 관리장치(3)의 유효무효 설정수단(61)에서 유효로 설정한 암호장치를 평문통신으로 한다고 결정해도 좋다. 유효무효 설정수단(61)에서 무효로 설정한 암호장치는 암호통신을 실행한다. 유효무효 설정수단(61)에서 설정한 유효무효정보는 관리장치(3)에서 암호장치(41), (42)의 유효무효 판정수단(713), (723)으로 송신되고, 각 암호장치의 유효무효 판정수단이 암호통신으로 할지 평문통신으로 할지를 판정한다.

또, 도2의 암호화시스템의 블록도에 있어서, 관리장치(3)의 유효무효 설정수단(61)과 암호장치(41), (42)의 유효무효 판정수단(713), (723)을 생략해도 좋다. 이 경우, 암호장치(41), (42)의 모드스위치(712), (722)의 온/오프에 의해 암호통신으로 할지 평문통신으로 할지를 설정한다.

또, 도9에 관리장치(3a)가 섹션키를 배송하지 않는 경우의 블록도를 도시한다.

도9에 도시한 바와 같이 관리장치(3a)는 도2에 도시한 섹션키 송신개시 검출수단(33), 섹션키 암호화수단(34), 섹션키 송신수단(35)을 생략한다. 암호장치(41a), (42a)는 섹션키 복호수단(411), (421), 섹션키 수신수단(412), (422)를 생략한다. 이 경우, 관리장치(3a)에 있어서 통신장치 그룹 기억수단(37)에 기억된 그룹마다 섹션키를 섹션키 생성수단(31)에 의해 생성한다. 관리장치(3a)에서 생성된 섹션키는 네트워크를 사용한 통신에 관계없이 각 암호장치의 섹션키 기억수단에 기억된다. 다른 기능은 상술한 설명과 동일하다.

도10에는 도2에 도시한 암호화시스템의 관리장치가 없는 경우를 도시한다.

LAN1에 암호장치(41b), (42b)를 거쳐 통신단말(21), (22)가 접속된다. 암호장치 및 통신단말은 도시하고 있지 않지만, 다른 것에도 접속되어 있다. 암호장치(41b), (42b)는 섹션키 기억수단(711), (721), 암호처리수단(413), (423), 데이터 송수신수단(414), (424), 모드스위치(712), (722)로 이루어진다. 통신단말(21), (22)는 도2와 마찬가지로이다. 섹션키는 섹션키 생성수단과 마찬가지로의 기능을 갖는 처리장치에 있어서 작성되고, 각각 암호장치(41b), (42b)의 섹션키 기억수단(711), (721)에 입력되고 기억된다. 섹션키의 동일 암호장치끼리가 동일 그룹으로 된다. 모드스위치(712), (722)의 스위치의 온/오프에 의해 암호통신으로 할지 평문통신으로 할지가 결정된다.

실시형태2

이 실시형태는 통신상대로 되는 통신장치, 어플리케이션, 통신방향에 따라 암호통신으로 할지 평문통신으로 할지의 암호화조건을 설정할 수 있는 암호화 시스템에 대해서 기술한다.

또, 여러개의 섹션키를 1대의 암호장치에 보유하고 통신상대, 어플리케이션, 통신방향에 따라 어떠한 섹션키를 사용할지의 암호화조건을 설정할 수 있는 암호화시스템에 대해서 기술한다.

도11은 이 실시형태에 있어서의 암호화시스템의 블록도이다.

LAN1에 키관리장치(6)과 암호장치(81), (82)가 접속되어 있다. 키관리장치(6)에는 입출력장치(5)가 접속되어 있다. 암호장치(81), (82)에는 통신단말(21), (22)가 접속되어 있다. 키관리장치(6)은 섹션키 생성수단(31), 섹션키 관리수단(32), 섹션키 송신개시 검출수단(33), 섹션키 암호화수단(34), 섹션키 송신수단(35), 통신장치 그룹 기억수단(37), 암호화조건 설정수단(62)로 이루어진다. 암호장치(81)은 섹션키 복호수단(411), 섹션키 수신수단(412), 암호처리수단(413), 데이터 송수신수단(414), 섹션키 기억수단(711), 암호화조건 기억수단(811), 조건판정수단(812)로 이루어진다. 암호장치(82)도 마찬가지로의 구성이다. 통신단말(21), (22)는 도2와 마찬가지로의 구성이다. 암호장치의 암호화조건 기억수단(811), (821)은 통신데이터의 암호화에 관한 암호화조건을 기억한다. 암호화조건으로서 통신상대로 되는 통신장치, 어플리케이션, 통신방향에 따라 암호통신으로 할지 평문통신으로 할지를 설정한다. 또, 여러개의 섹션키를 암호장치에 보유하고, 통신상대, 어플리케이션, 통신방향에 따라 어떠한 섹션키를 사용할지를 암호화조건에 의해 설정한다. 암호화조건 기억수단(811), (821)은 이들 암호화조건을 기억한다. 암호화조건을 설정하는 것은 키관리장치(6)의 암호화조건 설정수단(62)에 의해 키관리장치(6)의 관리자가 각각의 암호장치에 관해 조건을 설정하고 각 암호장치로 송신한다. 또는 키관리장치(6)의 암호화조건 설정수단(62)는 생략하고, 각각의 암호장치에 있어서의 암호화조건 기억수단(811), (821)에 있어서 각각의 암호장치의 사용자가 암호화조건을 암호화조건 기억수단(811), (821)에 설정해도 좋다. 조건판정수단(812), (822)는 암호화조건 기억수단(811), (821)에 기억된 암호화조건과 수신한 통신데이터의 통신상대로 되는 통신장치, 통신방향, 어플리케이션, 또 여러개의 섹션키가 있는 경우에는 섹션키에 의해 평문통신으로 할지 암호통신으로 할지 또는 어떠한 섹션키를 사용할지를 판정한다.

도12는 이 실시형태에 있어서의 암호화시스템을 이용한 네트워크 시스템의 예이다.

서버(91), WWW(World Wide Web) 대리서버(92), 메일서버(94)가 라우터(14)를 거쳐서 인터넷(16)에 연결되어 있다. 또, WWW(93)이 인터넷(16)에 접속되어 있다. 암호장치(81), (82)가 LAN1에 접속되어 있다. 암호장치(81)은 통신단말(21), (22)를 접속한다. 암호장치(82)는 통신단말(23), (24)를 접속한다. LAN1에는 그 밖에도 암호장치 및 통신단말이 접속되어 있지만 도면에서는 생략한다. 암호장치(81), (82)는 그룹A에 속한다.

도12의 네트워크에 있어서 암호장치(81)의 암호화조건을 다음과 같이 설정한다.

기본패스 : 어플리케이션(전체), 암호

특예1 : IP어드레스(메일서버) & 어플리케이션(메일) & 통신방향(출), 투과

특예2 : IP어드레스(WWW 대리서버) & 어플리케이션(http) & 통신방향(출), 투과

특예3 : IP어드레스(서버) & 어플리케이션(내임서버), 투과

상기의 암호화조건은 기본패스와 특예패스가 있지만, 특예패스에서 기술한 조건쪽이 우선순위는 높다. 통신의 통신은 기본패스에서 지정된 암호화조건에 따른다. 그러나, 특예1, 2, 3에서 지정된 암호화 조건에 적합한 통신데이터의 경우, 특예패스에서 기술한 조건을 우선한다. 도12를 사용해서 설명하면, 통신단말(21) 또는 (22)에서 그룹A내의 통신단말(23) 또는 (24)로 통신을 보내는 경우에는 기본패스의 암호화조건에 따라 모든 어플리케이션의 통신데이터에 대해서 암호화한다. 이 통신의 흐름을 도면에서는 점선으로 나타낸다. 통신단말(21), (22)에서 메일서버(94)로 메일을 보내는 경우, 특예1의 암호화조건에 적합하여 투과 즉 평문통신으로 된다.

통신단말(21), (22)에서 WWW 대리서버(92)로 어플리케이션(http)의 사용자데이터를 송신하는 경우, 특예2에 적합하여 평문통신으로 된다.

통신단말(21), (22)에서 서버(91)로 어플리케이션(내임서버)에 의해 통신데이터를 송수신하는 경우, 특예3에 따라 평문통신으로 된다. 특예3에서는 통신방향을 지정하고 있지 않으므로, 송수신하는 양방향의 데이터에 대

해서 루과, 즉 평문통신으로 된다. 또한, 암호장치(82)의 암호화조건은 암호장치(81)과 달라도 좋다. 또, 암호장치에 여러개의 통신단말이 접속되어 있는 경우에는 접속된 단말마다 다른 암호화조건(특에패스)을 설정해도 좋다.

또한, 기본패스, 특에패스에 대해서는 후술하는 실시형태에서 더욱 상세하게 설명한다.

이와 같이 1대의 암호장치에 의해 그룹내의 통신은 암호화하여 공공적인 메일서비스나 WWW 서비스를 평문으로 받을 수 있다.

도13은 이 실시형태에 있어서의 암호화시스템의 다른 네트워크예이다.

인터넷(16)에 WWW서버(95)와 메일서버A(96)이 접속되어 있다. 라우터(14)를 거쳐 2개의 LAN1이 접속되고, 한쪽의 LAN1에 암호장치(81)이 접속된다. 암호장치(81)에는 통신단말(21)과 사내 메일서버(97)이 접속된다. 또, 다른 한쪽의 LAN1에는 암호장치(82)가 접속된다. 암호장치(82)에는 사내 메일서버(98)과 통신단말(22)가 접속된다. 암호장치(81)과 (82) 및 통신단말(21), (22), 사내 메일서버(97), (98)은 동일 그룹에 속한다.

도13은 네트워크에 있어서 암호장치(81)의 암호화조건을 다음과 같이 설정한다.

기본패스 : 어플리케이션(메일+WWW), 루과

특예1 : IP어드레스(모든 사내의 암호장치의 어드레스) & 어플리케이션(전체), 암호

상기와 같이 암호화조건을 설정하면, 암호장치(81)을 통과하는 모든 사내 메일이나 사내의 어플리케이션 데이터는 암호화되고, 인터넷(16)에 접속된 공공의 메일서버A(96)의 메일이나 WWW 서버(95)와의 통신데이터의 수수는 루과, 즉 평문통신으로 된다.

이와 같이 인터넷에 접속된 통신장치라도 암호장치를 거치는 것에 의해 동일 사내에서 1개의 그룹을 형성하고, 통신데이터의 수수는 암호화할 수 있다. 그 때문에 인터넷을 거친 통신이더라도 도청을 방지할 수 있다.

도14는 암호화시스템을 사용한 다른 네트워크예이다.

LAN/WAN(15)에 LAN1이 라우터(14)를 거쳐 3개 접속되어 있다. LAN1에는 암호장치(81)~(85)가 접속되어 있다. 통신단말(21)~(29)는 암호장치에 접속되어 있다. 통신단말(20)은 암호장치를 거치지 않고 LAN1에 접속되어 있다. 인사파일서버(99)는 암호장치(83)에 접속되어 있다.

도14의 네트워크에 있어서 암호장치(84)의 암호화조건을 다음과 같이 설정한다.

기본패스 : 어플리케이션(전체), 섹션키A에 의해 암호

특예 : IP어드레스(인사파일서버) & 어플리케이션(전체), 섹션키B에 의해 암호

도14에 있어서, 그룹A는 섹션키A에 의한 그룹이다. 예를 들면, 기술부의 그룹으로 한다. 그룹B는 섹션키B에 의한 그룹이다. 예를 들면 이것을 인사부로 한다. 그룹B에는 인사파일서버(99)가 있어 일반적인 액세스는 금지하고자 한다. 상기와 같이 암호화조건을 설정하면 통신단말(27)에서 섹션키A를 사용하면, 그룹A내의 모든 통신단말과 모든 어플리케이션에 대해서 통신데이터를 송수신할 수 있다. 통신단말(27)에서는 섹션키B를 사용해서 인사부, 즉 그룹B의 인사파일서버(26)과 모든 어플리케이션에 관해 통신데이터를 송수신할 수 있다. 그 때문에 통신단말(27)의 사용자를 인사권이 있는 임원으로 한다

이와 같이 암호장치에 여러개의 섹션키를 보유하고, 암호화조건에서 어떠한 섹션키를 사용할지 설정하는 것에 의해 여러가지 그룹의 조합을 중복해서 작성할 수 있다. 그 때문에 섹션키에 의한 암호화조건의 설정에 의해 도청방지 및 액세스제어가 가능하여 인사과나 임원밖에 액세스할 수 없는 인사정보서버 등을 사내 LAN에 접속할 수 있다.

도15는 암호화시스템을 사용한 다른 네트워크예이다. WAN(17)은 라우터(14)를 거쳐 2개의 LAN1과 접속되

어 있다. 각각의 라우터(14)의 LAN1측에 암호장치(81)과 (82)를 접속한다 이것에 의해 예를 들면 사내전체를 1개의 그룹, 그룹A로 할 수 있다. 2개의 LAN1에는 암호장치(83)과 (84)가 각각 접속되어 있다. 암호장치(83)과 (84)에는 통신단말(23), (24), (27), (28)이 접속되어 있다. 그러나, 더 많은 통신단말을 암호장치에 각각 접속해도 좋다.

또, LAN1에는 암호장치를 거치지 않고 통신단말(21), (22), (25), (26)이 접속되어 있다. 그러나, 더 많은 통신단말을 접속해도 좋다. 암호장치(83)과 (84) 및 암호장치에 접속된 통신단말에 의해 그룹B가 형성된다. 그룹B를 예를 들면 인사부로 한다. 그룹B는 그룹A에 속한다. 그러나, 암호장치(83), (84)를 거치지 않는 그룹A의 통신단말(21), (22), (25), (26)에서는 그룹B의 통신단말(23), (24), (27), (28)과 통신데이터의 수수를 하는 것은 불가능하다.

또, 통신단말(21), (22), (25), (26)은 서로 통신데이터를 송수신할 수 있지만, 통신데이터는 암호화되지 않는다. 암호화되는 것은 예를 들면 통신장치(21)이 통신장치(25)로 통신데이터를 송수신하고자 하는 경우, 통신장치(21)측의 LAN1에 접속된 암호장치(81)에서 암호화되고 WAN(17)을 거쳐 암호장치(82)에서 복호될 때까지이다. 암호장치(82)에서 복호된 통신데이터는 평문통신에 의해 통신단말(25)에 도달한다. 즉, WAN(17)과 같은 공중망을 통과할 때에 암호화되어 도청을 방지할 수 있다.

이와 같이 암호장치를 배치하는 것에 의해 도청을 방지할 수 있으므로 종래 전용선에서 밖에 구축할 수 없었던 시스템이 공중망을 이용할 수 있다.

도16은 어플리케이션과 섹션키에 의해 암호화조건을 결정하는 것에 의해 중복된 여러개의 그룹화가 가능한 것을 설명하는 도면이다.

암호장치(81)~(83)이 LAN1에 접속되어 있다. 암호장치(81)에서는 어플리케이션(1)~(4)와 (6)을 실행한다. 암호장치(82)에서는 어플리케이션(1), (3), (5), (6)을 실행한다. 암호장치(83)에서는 어플리케이션(1), (2), (4)~(6)을 지정한다. 동일 번호의 어플리케이션이 등록되어 있는 암호장치 사이에서는 동일 섹션키로 통신데이터를 암호화/복호하는 것으로 한다. 이것에 의해 어플리케이션(1), (6)이 지정되어 있는 암호장치(81)~(83)에서 그룹A가 형성된다. 어플리케이션(2), (4)가 지정되어 있는 암호장치(81), (83)에서 그룹B가 형성된다. 어플리케이션(3)이 지정되어 있는 암호장치(81), (82)에서 그룹C가 형성된다. 어플리케이션(5)가 지정되어 있는 암호장치(82)와 (83)에서 그룹D가 형성된다.

이와 같이 암호화조건의 지정 방식에 의해 상기와 같이 3대의 암호장치를 여러개로 조합하여 중복된 여러개의 그룹을 형성할 수 있다. 또한, 이 예에서는 어플리케이션을 예로 했지만, 통신프로토콜 타입에 의해 그룹화해도 좋다.

암호장치에 1개의 섹션키밖에 보유할 수 없는 경우, 암호장치와 섹션키가 1대 1로 대응하므로, 섹션키를 어느 암호장치에 갖게 하는 것에 의해 암호장치의 그룹화를 한다. 이 경우, 물리적 네트워크의 그룹을 형성할 수 있다.

암호장치에 여러개의 섹션키를 보유할 수 있는 경우에는 어플리케이션이나 통신프로토콜 등의 기능과 섹션키의 조합에 의해 1대의 암호장치가 중복해서 여러개의 그룹에 속할 수 있다. 이것은 물리적 네트워크 그룹에 대해 논리적 네트워크 그룹이라고 말할 수 있다.

도17은 도11에서 관리장치(6a)가 섹션키는 생성하지만, 암호장치(81a), (82a)에 네트워크를 거쳐서 배송하지 않는 경우의 블록도이다. 암호화조건의 설정 및 암호화조건의 판정은 상술한 바와 같다.

도18은 도11에 있어서 관리장치를 생략한 경우의 블록도이다.

각 암호장치에서 보유하는 섹션키는 관리장치(6)의 섹션키 생성수단(31)과 동등한 기능을 갖는 처리장치

에서 작성하고, 암호장치(81b)의 섹션키 기억수단(711)에 입력해서 기억된다. 이 경우도 여러개의 섹션키를 작성하고, 섹션키 기억수단(711)에 기억시키는 것은 가능하다. 암호장치(81b), (82b)는 섹션키 기억수단(711), (721), 암호처리수단(413), (423), 데이터 송수신수단(414), (424), 암호화조건 기억수단(811), (821), 조건판정수단(812), (822)로 이루어진다. 암호화조건은 각각 암호장치의 사용자가 암호화조건 기억수단(811), (821)에 기억한다. 암호화조건에 의한 논리적 네트워크 그룹의 형성은 상기 설명과 마찬가지로이다.

또한, 상기 실시형태에서 기술한 모드스위치를 암호장치에 구비해도 좋다. 이 경우, 암호화조건이 어떠한 것이라도 모드스위치가 온이면 평문통신으로 전환되는 것으로 한다.

이상과 같이 이 암호화시스템을 사용하는 것에 의해 전용선에서 밖에 구축할 수 없었던 도청방지시스템을 공중망이나 인터넷을 이용해서 구축할 수 있다.

또, 네트워크를 사용한 정보서시스템에 있어서 암호키를 가진 사용자만이 액세스할 수 있는 그룹화를 도모할 수 있다.

또, 인사과나 임원밖에 액세스할 수 없는 인사정보서버 등을 사내 LAN에 접속할 수 있다. 이 경우, 암호화조건의 설정에 의해 일반 사용자가 인사정보서버를 도청할 수 없고 액세스할 수도 없다.

또, 암호화조건의 기능(통신프로토콜, 어플리케이션)과 섹션키 지정의 방식에 의해 여러개의 중복된 논리그룹을 동일 네트워크상에 구축할 수 있다.

실시형태3

이 실시형태는 1대의 암호장치에 통신단말이 접속되는 경우, 통신단말을 접속하는 포트마다 암호화를 위한 조건을 기본패스와 특예패스에 의해 설정할 수 있는 암호화시스템에 대해서 기술한다.

도19는 이 실시형태에서 사용하는 네트워크시스템을 도시한 도면이다.

도면에 있어서, 암호장치(81)~(84)는 통신단말이 1대 접속되는 NODE형 암호장치이다. 암호장치(51), (52)는 통신단말이 여러대 접속되는 HUB형 암호장치이다. 암호장치(81), 암호장치(51), 암호장치(82)는 이들 암호장치에 접속되는 통신단말(20)~(23), (25)와 함께 그룹A를 형성한다. 암호장치(83), (84)와 암호장치(52)는 각각에 접속되는 통신단말(26)~(29)와 함께 그룹B를 구성한다. 관리장치(7)는 LAN1에 접속되고, 암호장치(81)~(84)와 암호장치(51), (52)의 암호화/복호에 사용하는 섹션키를 생성하고, 각 암호장치에 배포한다. 또, 통신단말(24)는 평문통신에만 실행할 수 있는 단말이다.

도20에 1대의 암호장치에 1대의 통신단말이 접속되는 NODE형 암호장치(81)을 도시한다.

암호장치(81)에는 평문포트와 암호포트가 있고, 평문포트에는 통신단말(20)이 1대 접속된다. 통신단말(20)과 암호장치(81) 사이를 흐르는 데이터는 암호화되지 않는 평문이다. 암호장치(81)의 암호포트는 LAN1에 접속된다. 암호port를 흐르는 데이터는 암호화된 데이터인 경우도 있고, 평문인 경우도 있다. NODE형 암호장치는 접속 제한으로 해서 평문포트측에 1대의 통신단말만이 접속되고, 다른 HUB나 브리지/라우터의 접속은 금지이다. 또, 암호화조건으로 지정하는 통신방향은 평문포트에서 암호포트로 데이터가 흐르는 방향을 (출), 즉 출방향으로 정의한다.

도21에 1대의 암호장치에 여러대의 통신단말이 접속되는 HUB형 암호장치(51)을 도시한다.

암호장치(51)의 평문포트에는 통신단말(21), (22), (23)이 접속된다. 암호장치(51)의 암호포트는 LAN1에 접속된다. HUB형 암호장치의 접속 제한으로서는 평문포트측에는 여러개의 포트를 구비하고, 1개의 포트에 1대의 단말만이 접속되고 다른 HUB나 브리지/라우터의 접속은 금지이다. 암호화조건에 의해 사용하는 통신방향(출)은 도면에 도시한 바와 같이 평문포트에서 암호포트로 흐르는 방향으로 한다.

도22는 이 실시형태에서 사용하는 관리장치(7)와 암호장치(81), 암호장치(51), 통신단말(20)~(23)의 블록도

이다.

키관리장치(7)은 상기 실시형태에서 기술한 도11에 있어서의 키관리장치(6)에 포트조건 설정수단(63)이 부가된 것이다. 암호장치(51)은 통신단말(21)~(23)이 접속되는 HUB형 암호장치이다. 암호장치(51)은 도11에 있어서의 암호장치(82)의 암호화조건 기억수단(821)이 포트조건 기억수단(921)로 치환된 것이다. 포트조건 기억수단(921)은 통신단말을 접속하는 포트마다 상기 실시형태에서 기술한 기본패스와 특예패스를 포트조건으로서 기억한다. 조건판정수단(822)는 포트조건 기억수단(921)에 설정되어 있는 포트조건과 통신단말(21)~(23)에서 입력된 통신데이터의 조건(통신데이터를 사용하는 어플리케이션, 통신방향, 통신상대로 되는 통신장치)을 비교하고, 포트조건 기억수단(921)에 기억된 기본패스와 특예패스중의 어느 하나의 패스를 사용할지 판정하고, 기본패스 또는 특예패스에 설정된 섹션키에 의해 암호화할지 또는 평문통신으로 할지 결정한다.

암호장치(81)은 통신단말(20)을 1대 접속하는 NODE형 암호장치이다. 입출력장치(5)와 암호장치(81)과 통신단말(20)~(23)은 도11과 마찬가지로이다.

키관리장치(7)에 있어서의 포트조건 설정수단(63)은 키관리자가 HUB형 암호장치의 포트조건을 설정하고, 대상으로 되는 HUB형 암호장치(51), ...에 있어서의 포트조건 기억수단(921) ...에 배포한다. 그러나, 암호장치(51), ...에 있어서 각각 포트조건을 설정하고, 포트조건 기억수단(921) ...에 설정되면 키관리장치(7)에 있어서의 포트조건 설정수단(63)은 생략해도 좋다. 그러나, 키관리장치(7)의 포트조건 설정수단(63)에서 암호장치의 포트조건을 설정하는 것에 의해 일괄관리가 가능하게 된다.

섹션키 기억수단(711), (721)은 키관리장치(7)의 섹션키 생성수단(31)에 의해 생성된 키와 암호화조건 기억수단(811) 또는 포트조건 기억수단(921)에 설립되는 키의 식별명칭과의 대응을 기억한다. 예를 들면, 암호화조건 기억수단(811)에 기억되는 기본패스와 특예패스에서 키A, 키B, 키C로 지칭하는 것으로 한다. 섹션키 기억수단(711), (721)에는 섹션키의 식별명칭, 키A, 키B, 키C와 각각에 대응하는 키관리장치(7)에서 배송된 섹션키를 기억한다.

이와 같이 하는 것에 의해 암호화조건과 포트조건을 설정하는 키관리자가 실제의 섹션키를 알 필요가 없다. 또, 섹션키의 비밀성을 유지하기 위해 정기적으로 섹션키를 키관리장치(7)에서 생성하고 변경하는 경우, 암호화조건과 포트조건에 섹션키의 식별자로 지정하므로 암호화조건과 포트조건을 섹션키의 갱신시마다 변경할 필요가 없다.

도23에 암호화조건 기억수단(811)에 기억시키는 암호화조건의 예를 도시한다. 도23의 암호화조건을 다음에 기술한다.

기본패스 : 어플리케이션(전체), 키A

특예패스0 : 수신지 IP어드레스(전체) & 어플리케이션(메일), 루과

특예패스1 : 수신지 IP어드레스(통신단말26) & 어플리케이션(AP11) & 통신방향(출), 키B

이와 같이 암호화조건으로서는 기본패스와 특예패스를 기억할 수 있다.

기본패스는 디폴로(default)로서 취급되는 패스로서, 특예패스와 합치하지 않는 통신은 모두 기본패스로 취급된다. 그 때문에 수신지 IP어드레스의 지정은 불가능하다.

한편, 특예패스는 수신지 IP어드레스를 반드시 설정하고, 특예패스에서 설정된 조건과 합치하는 통신은 해당 특예패스에서 설정된 섹션키에 의해 암호화된다. 또는 루과설정된 경우에는 암호화하지 않고 평문 그대로 암호장치에서 출력된다.

기본패스와 특예패스에서는 특예패스는 지정하지 않아도 좋다. 즉, 암호화조건은 적어도 기본패스를 설정하지 않으면 안된다. 또한, 기본패스 및 특예패스와 합치하지 않는 통신은 모두 폐기된다.

다음에, 기본패스와 특예패스의 특징을 각각 기술한다.

기본패스는 NODE형 암호장치에서는 평문포트가 1개이므로 1개 설정할 수 있다. 기본패스에서는 수신지 IP어드레스는 지정할 수 없지만 어플리케이션필터, 통신방향필터, 섹션키를 지정할 수 있다.

어플리케이션필터는 특정 어플리케이션명의 지정이 가능하며, 그 밖에 전체 통과 또는 전체 폐기의 지정이 가능하다.

또, 데이터가 암호장치의 평문포트에서 암호포트로 출력할지 또는 입력할지에 의한 통신방향필터의 설정이 가능하다. 통신방향은 도20, 도21에 도시한 바와 같이 평문포트에서 암호포트로 데이터가 흐르는 방향을 출방향(출)로 한다. 반대로, 암호포트에서 평문포트를 데이터가 흐르는 경우, 입방향(입)으로 한다. 또, 출방향 및 입방향을 합친 양방향의 지정이 가능하다. 양방향을 지정하는 경우에는 기본패스 및 특예패스에 통신방향을 명기하지 않으면 양방향 취급으로 된다.

섹션키는 어플리케이션필터, 통신방향필터의 각 조건과 합치한 통신을 암호화하는 경우에 사용한다. 섹션키는 기본패스인 경우, 암호장치가 속하는 그룹의 키로 고정시킨다. 또, 섹션키를 지정하지 않고 투과설정(평문 통신)으로 하는 것도 가능하다.

특예패스는 여러종류 설정하는 것이 가능하고, 이 실시형태에서는 1대의 암호장치에서 최대 64종류를 설정할 수 있다. 특예패스에서는 수신지 IP어드레스필터, 어플리케이션필터, 통신방향필터, 섹션키를 지정할 수 있다.

특예패스에서는 수신지 IP어드레스를 지정하지 않으면 안된다. 또, IP어드레스의 유효비트길이라도 아울러 지정한다.

암호화조건의 통신상대는 조건설정으로서 IP어드레스와 IP어드레스의 유효비트길이라는 2항목을 설정한다. IP어드레스는 4개의 숫자를 도트(.)으로 구획해서 표현한다. 각 수치는 0~255까지의 범위를 취할 수 있다. 0~255의 수치는 2진수로 표현하면 8비트로 나타낼 수 있으므로 유효비트길이에 따라(8비트×4) 자리수중 어디까지의 비트를 그대로 사용할지를 지정한다. 유효비트길이에에서 범위의로 된 비트는 0이라고 간주한다. 예를 들면, 133. 141. 70. 151이라는 IP어드레스이고 유효비트길이=32비트인 경우에는 통신상대로 되는 통신장치는 1개뿐으로 133. 141. 70. 151의 IP어드레스를 갖는 통신장치로 된다.

그러나, 동일 133. 141. 70. 151라는 IP어드레스이고 유효비트길이=24비트로 하면, 133. 141. 70. 0~133. 141. 70. 255까지의 256종류의 IP종류의 IP어드레스 중 어느 하나의 IP어드레스를 갖는 여러개의 통신장치가 통신상대로 된다. 이와 같이 IP어드레스의 유효비트길이 지정에 의해 통신상대로 되는 통신장치는 1개이거나 또는 여러개로 한다.

특예패스의 어플리케이션필터, 통신방향 필터에 관해서는 기본패스와 동일 사양이다.

섹션키는 수신지 IP어드레스필터, 어플리케이션필터, 통신방향 필터의 각 조건과 합치한 통신을 암호화한다. 섹션키는 섹션키 기억수단(711)에 여러개의 섹션키를 기억시키는 것에 의해 여러개의 섹션키중에서 1개를 선택해서 특예패스에 지정할 수 있다. 섹션키는 특예패스마다 1개 지정한다. 또는 평문통신으로 하는 통과설정으로 하는 것도 가능하다.

또, 특예패스에서는 수신지 IP어드레스를 지정한다는 특성에 의해 예를 들면 IP 브로드캐스트 어드레스는 취급할 수 없다. 즉, 브로드캐스트를 사용하는 어플리케이션은 특예패스에서는 취급할 수 없어 기본패스중에서 취급하게 된다.

도24에 포트조건 기억수단(921)에 기억시키는 포트조건의 예를 도시한다.

도24에 있어서의 포트조건을 다음에 기술한다.

포트1

기본패스1 : 어플리케이션(전체), 키A

포트2

기본패스2 : 어플리케이션(메일), 루과

특예패스1 : 수신지 IP어드레스(통신단말(26)) & 어플리케이션(AP11) & 통신방향(출), 키B

포트3

기본패스3 : 어플리케이션(AP22) & 통신방향(입), 키A

특예패스1 : 수신지 IP어드레스(통신단말(26)) & 어플리케이션(AP11) & 통신방향(출), 키B

특예패스2 : 수신지 IP어드레스(통신단말(28)) & 어플리케이션(SPPR) 키C

HUB형인 암호장치(51)은 여러개의 포트를 구비하고, 도22의 예에서는 3대의 통신단말(21)~(23)이 접속되어 있다. 그 때문에 포트1, 포트2, 포트3마다 각각 포트조건을 기억한다. 포트조건으로서는 기본패스와 특예패스를 지정할 수 있다.

기본패스와 특예패스의 특징은 상술한 바와 같지만, NODE형 암호장치와 HUB형 암호장치에서는 다음과 같은 차이점이 있다.

NODE형 암호장치에 있어서의 기본패스는 장치당 1개 지정한다. HUB형 암호장치에서는 포트마다 1개의 기본패스를 설정한다. 특예패스는 HUB형 암호장치에서 있어서는 여러개의 포트에서 공유가능하다.

기본패스와 특예패스에서는 특예패스는 지정하지 않아도 좋다. 즉, 포트조건은 각 포트마다 적어도 기본패스를 설정해야만 한다.

특예패스와 기본패스의 우선순위는 특예패스가 우선된다. 또, 특예패스가 여러개 있는 경우에는 특예패스 각각에 미리 우선순위를 부가해 둘 수도 있다. 이 실시형태에서는 암호조건 기억수단, 포트조건 기억수단에 기억시키는 특예패스의 순번에 따라 우선순위를 부가한다.

도25에 도24에 도시한 포트조건을 예로 포트조건에 있어서의 기본패스와 특예패스의 관계를 기술한다.

도25에 도시한 모식도에서는 포트1은 기본패스뿐이다. 포트2는 기본패스와 특예패스1, 포트3은 기본패스와 2개의 특예패스 1, 2를 갖는다. 또, 특예패스1은 포트2와 포트3에서 공유하고 있는 것을 나타내고 있다. 또, 파이프 도중에 삽입되어 있는 타원형의 골라낸 것에 해당하는 부분이 각종 선택처리를 나타내고 있다. 도면의 타원형으로 ()내에 기재한 것은 도24의 포트조건이다. 예를 들면, 특예패스(2)를 예로 들면 수신지 IP어드레스 필터에 있어서의 (28)은 통신단말(28)을 나타낸다. 어플리케이션필터(SPPR)은 어플리케이션SPPR을 나타낸다. 통신방향 필터에 있어서의 (양)은 통신방향이 양방향인 것을 나타낸다. 섹션키(C)는 섹션키의 식별자로서 키C를 나타낸다.

또, 기본패스 1, 3에서 지정하는 섹션키는 암호장치가 속하는 그룹의 섹션키A로서, 고정적이다. 기본패스2에는 루과를 설정한다.

기본패스와 특예패스를 이와 같이 설정할 수 있으므로, 암호화하는 것에 의한 안전강화와 함께 사용자의 편리성을 고려해서 몇가지의 선택성을 제공할 수 있다. 예를 들면, 통상 암호세계에 있는 사용자가 네트워크를 평문으로 운용하고자 하는 요망에 응답해서 뉴스서버와의 통신만 예외적으로 평문에서 실행하는 것이 가능하게 된다. 또, 특예패스를 사용하여 그룹에 부가된 섹션키 이외의 섹션키를 지정할 수 있으므로 미리 설정된 그룹을 논리그룹으로 하면, 이 논리그룹에 속하면서 새로운 논리그룹을 형성할 수 있다. 새로운 논리그룹을 형성하는 조건은 수신지 IP어드레스, 어플리케이션, 통신방향, 섹션키이며, 이들 조합에 의해 설정할 수 있다.

도26에 도19에 도시한 네트워크시스템에 있어서 암호장치(81), (51)에서 도23, 도24에 도시한 암호화조건과

포트조건을 설정하는 것에 의해 형성되는 새로운 논리그룹을 도시한다.

그룹A에 속하는 통신단말(20), (22), (23)은 특정 어플리케이션(AP11)인 경우, 통신단말(26)로 통신데이터를 출력할 수 있다. 통신단말(20), (22), (23)은 그룹A에 속하지만, 특예패스1을 설정하는 것에 의해 그룹B의 통신단말(26)과 새로운 논리그룹1을 형성한다. 논리그룹1은 어플리케이션(AP11)을 통신단말(20), (22), (23)에서 처리할 때에 형성되는 그룹이다. 또, 통신방향이 통신단말(20), (22), (23)에서 통신단말(26)으로 출력되는 경우에만 형성되는 그룹이다.

논리그룹2는 도24의 포트3에 있어서의 특예패스1에서 설정된 조건에 의해 생기는 그룹이다. 이 경우, 논리그룹2는 통신단말(23)에 있어서 어플리케이션(SPPR)이 실행될 때 통신단말(28)과 데이터가 수신을 하는 경우에 생기는 그룹이다. 이와 같이 특예패스의 설정에 의해 미리 정해진 그룹을 넘어서 새로운 논리그룹을 형성하는 것이 가능하게 된다.

또, 특예패스의 설정방식에 의해 예를 들면 그룹A중에 1이상의 서브그룹을 형성하는 것도 가능하게 된다.

또, 1대의 암호장치에 여러대의 통신단말이 접속되어 있더라도 포트마다 포트조건을 설정하는 것에 의해 각 통신단말마다 다른 사용방법이 가능하게 된다. 예를 들면, 도24의 예인 경우 통신단말(21)은 그룹A에만 속한다. 통신단말(22)는 기본적으로는 어플리케이션(메일)을 위한 통신단말로 하고, 다른 어플리케이션(메일)을 실행하는 통신단말과 그룹분류에 관계없이 데이터교환이 평문으로 가능하게 된다. 또, 어플리케이션(AP11)을 실행할 때, 통신단말(22)에서 통신단말(26)으로 데이터를 송신하는 단말로 된다.

통신단말(23)은 어플리케이션(AP22)을 실행하는 경우, 다른 통신단말에서 통신을 수신하는 단말로서 기본적으로 동작한다. 또, 어플리케이션(AP11)을 실행하고, 통신단말(26)으로 데이터를 송신하는 단말로 된다. 또, 어플리케이션(SPPR)을 실행할 수 있어 통신단말(28)과 통신의 수신을 실행할 수 있는 단말이다.

이와 같이 1개의 암호장치에 접속되어 있으면서 각 통신단말마다 각각 성격이 다른 역할을 분담하는 것이 가능하게 된다.

도27은 HUB형 암호장치를 사용한 통신형태의 예를 도시한 도면이다.

암호장치(51)하에 통신단말(21), (22)가 접속되고, 암호장치(52)하에 통신단말(23)과 DB서버(904)가 접속되고, 섹션키1에 의한 그룹1이 형성된다. 암호장치(53)하에 통신단말(24), (25)가 접속되고, 암호장치(54)하에 통신단말(26)과 DB서버(905)가 접속되고, 섹션키2에 의해 그룹2를 형성한다. 암호장치(51)~(54)는 HUB형 암호장치이다. 암호장치(51)의 포트(2)에 접속된 통신단말(22)가 EOA서버(901), 뉴스서버(902), WWW서버(903)은 평문 통신을 실행하고 또한, DB서버(905)와도 통신을 실행한다. 이 경우, 암호장치(51)에 도28에 도시한 포트조건(포트2만을 기재)을 설정한다.

기본패스 : 어플리케이션(전체), 키1

특예1 : 수신지 IP어드레스(aaa) & 어플리케이션(AP23) & 통신방향(출), 투과

특예2 : 수신지 IP어드레스(bbb) & 어플리케이션(A119) & 통신방향(출), 투과

특예3 : 수신지 IP어드레스(ccc) & 어플리케이션(T80) & 통신방향(출), 투과

특예4 : 수신지 IP어드레스(ddd) & 어플리케이션(AP1523) & 통신방향(출), 키2

여기서, aaa는 EOA서버의 IP어드레스이고, bbb는 뉴스서버의 IP어드레스이고, ccc는 WWW서버의 IP어드레스이며, ddd는 DB서버(905)의 IP어드레스이다. 기본패스는 그룹(1)에 속하는 것을 정의하고, 모든 어플리케이션에 대해서 또한 양방향통신에 대해서 섹션키1에 의해 암호화/복호를 실행하는 것을 의미한다. 특예패스1은 EOA서버와 평문통신을 실행하기 위한 설정이다. 특예패스2는 뉴스서버와 평문통신을 실행하기 위한 설정이다. 특예패스3은 WWW서버와 평문통신을 실행하기 위한 설정이다. 특예패스4는 DB서버(905)와 섹션키2에 의

해 암호화통신을 실행하기 위한 설정이다.

도29에 LAN에 접속하는 암호장치를 도시한다. LAN에 접속하는 암호장치(501)은 평문포트에서 입력된 암호화되어 있지 않는 데이터를 암호화하고, 암호포트에서 출력한다. 평문포트측의 접속에 제한은 없다.

도30과 도31에 LAN에 접속하는 암호장치(501)의 설치예를 도시한다.

도30에서는 라우터(142)와 광역망에 접속된 라우터(141)측에 암호장치(501)의 암호포트를 접속한다. 암호장치(501)의 평문포트에는 라우터(143)과 브리지(151)이 접속된다. 라우터(143)과 브리지(151)에서 입력되는 암호화되어 있지 않는 데이터가 암호장치(501)의 평문포트에 입력되고, 암호장치(501)에서 암호화되어 암호포트에서 출력된다. 암호화된 데이터는 라우터(141)을 거쳐서 광역망을 통과해 통신상대지로 통신된다. 또는 암호화된 데이터는 라우터(142)를 거쳐서 통신상대지로 통신된다.

도31은 LAN에 접속하는 암호장치(501), (502)의 제2설치예이다.

광역망에 라우터(141)이 접속되고, 라우터(141)에 이서넷(ether net) 스위치(131), (132)가 접속된다. 이서넷 스위치(131)의 1개의 포트에 LAN에 접속하는 암호장치(501)의 암호포트가 접속된다. 암호장치(501)의 평문포트가 일반 HUB(121)에 접속된다. 암호장치(502)에 관해서도 마찬가지이다. 일반 HUB(121) 또는 (122)에서 입력되는 암호화되어 있지 않는 데이터가 암호장치(501) 또는 (502)의 평문포트에 입력되고, 암호화되어 암호포트에서 이서넷 스위치(131) 또는 (132)로 출력된다. 암호장치(501), (502)의 암호포트측, 즉 이서넷 스위치(131), (132)와 라우터(141)을 거친 광역망측에서는 암호화된 데이터로 된다.

도32는 LAN에 접속하는 암호장치를 사용한 통신형태를 도시한 도면이다.

자회사A와 자회사B와 본사는 인터넷(16)을 거쳐 통신을 실행한다. 자회사A는 암호장치(501)을 인터넷(16)측의 라우터(143)에 접속한다. 자회사B는 암호장치(502)를 인터넷(16)측의 라우터(144)에 접속한다. 본사는 암호장치(503)을 인터넷(16)측의 라우터(145)에 접속한다. 이것에 의해 본사, 자회사A, 자회사B 사이에서 통신을 실행하는 경우, 암호장치(501), (502), (503)에 의해 인터넷측에서는 통신데이터가 암호화되므로 통신의 안전이 유지된다.

본사와 자회사A는 섹션키5를 사용한 통신을 실행한다. 본사는 자회사B와는 섹션키(6)를 사용해서 WWW서버 액세스만을 실행한다. 또, 본사에서 인터넷(16)상의 각종 공개서버(906)와는 평문으로 액세스를 실행하고자 한다. 이와 같은 통신형태를 실행할 때의 본사에 있는 암호장치(503)에서의 암호화조건을 도33에 도시한다.

기본패스1 : 어플리케이션(전체), 투과

특예1 : IP어드레스(aaa) & 어플리케이션(전체), 키5

특예2 : IP어드레스(bbb) & 어플리케이션(AP80) & 통신방향(출), 키6

여기서, aaa는 자회사A에 설치된 라우터(141)의 IP어드레스이다. bbb는 자회사B에 설치된 라우터(142)의 IP어드레스이다.

또한, LAN에 접속하는 암호장치에는 평문포트가 1개이므로 포트조건이 아닌 암호화조건을 기억시킨다.

이상과 같이 이 실시형태에서는 1대의 암호장치가 여러개의 포트를 구비하고, 각각의 포트에 통신단말이 여러개 접속되는 경우, 포트마다 암호화에 관한 포트조건을 기억시킬 수 있는 암호화시스템에 대해서 기술하였다. 이것에 의해 암호통신, 평문통신을 설정할 수 있음과 동시에 수신지 IP어드레스, 어플리케이션, 통신방향, 섹션키에 의해 포트마다 암호화하는 조건을 설정할 수 있다. 그 때문에 미리 설정된 통신장치로 이루어지는 논리그룹의 암호화통신 이외에 유연하게 수신지 IP어드레스, 어플리케이션, 통신방향, 섹션키에 의해 새로운 논리그룹을 설정할 수 있다. 또, 동일한 암호장치에 접속되는 통신단말이라도 각각의 포트조건을 변경할 수 있으므로 통신단말을 1대마다 다른 사용방법이 가능하여 사용자에게 있어서 사용하기 쉬운 암호화시스템을 제

공할 수 있다.

실시형태4

이 실시형태는 키관리장치와 암호장치와 통신단말에 의해 암호관리 도메인을 형성하고 여러개의 암호관리 도메인 사이에서 공통 섹션키를 갖는 것에 의해 다른 암호관리 도메인 사이의 암호화통신이 가능한 암호화시스템에 대해서 기술한다. 또, 암호화조건과 포트조건에 공통 섹션키를 설정하는 것에 의해 다른 암호관리 도메인에 속하는 통신단말로 이루어지는 논리그룹을 형성하는 암호화시스템에 대해서 기술한다.

도34는 이 실시형태에 있어서의 암호화시스템의 네트워크시스템을 도시한 도면이다.

암호관리도메인 A,B,C로 분류되고 각각 1대의 암호관리장치와 여러대의 암호장치와 여러대의 통신단말로 이루어진다. 암호관리도메인 사이는 라우터(14)와 LAN/WAN(15)에 의해 네트워크 접속되어 있다.

암호관리도메인 A~C는 통상 각각에 속하는 암호관리도메인(71)~(73)이 섹션키를 생성하고 관리하므로, 암호관리도메인 상호간의 암호화통신은 불가능하다. 그래서, 공통 섹션키를 여러개의 암호관리도메인에서 공유하는 것에 의해 암호관리도메인 사이의 암호화통신을 실행한다.

이 실시형태에서는 여러개 있는 키관리장치 중 1대의 키관리장치를 마스터키 관리장치로 하여 공통 섹션키를 생성하고, 다른 키관리장치로 배송한다. 여기서는 암호관리도메인A의 키관리장치(71)을 마스터키 관리장치로 하고, 공통 섹션키를 생성하여 배송하는 것으로 한다. 키관리장치(72) 및 키관리장치(73)을 키관리장치(71)에서 공통 섹션키를 수취하는 키관리장치로 한다.

또한, 공통 섹션키에 대해 암호관리도메인내에서 사용하는 섹션키를 로컬키라 부르는 것으로 한다.

도35에 키관리장치(71), (72)의 블록도를 도시한다.

키관리장치(71), (72)에는 도22에 도시한 키관리장치(7)에 섹션키 테이블(64)가 부가된다. 키관리장치(71), (72)에 있어서의 섹션키 생성수단(31)이 여러개의 섹션키를 생성하고, 섹션키 테이블(64)에 기억한다. 이 실시형태에서는 키관리장치(71)~(73)에서 각각 최대32개의 섹션키를 생성하는 것으로 한다.

도36에 섹션키 테이블(64)의 예를 도시한다. 섹션키 테이블(64)는 키번호, 키작성가부를 나타내는 허가플래그, 생성된 키, 그 키에 대한 속성을 기억하는 난이 있다. 키번호1~키번호32에 대응해서 공통 섹션키와 로컬키를 키의 난에 기억한다. 안전강화를 위해 일정시간마다 로컬키는 생성되고 갱신된다. 공통 섹션키는 갱신이 불가능하므로 허가플래그를 「비작성」(도면에서는 X로 나타낸다)으로 한다. 공통 섹션키에 대해 암호관리도메인A,B사이의 공통 섹션키인 것을 기억하기 때문에 속성란에 “공통(A,B)” 라고 기재되어 있다.

키관리장치(72)는 도22의 키관리장치(7)에 섹션키 테이블(64)에 부가해서 또 섹션키 수신수단(65)와 섹션키 복호수단(66)이 부가된 것이다. 섹션키 수신수단(65)와 섹션키 복호수단(66)은 키관리장치(71)에서 암호화되어 배송되는 공통 섹션키를 수신하고 복호한다.

또한, 키관리장치(71)~(73)의 통신장치그룹기억수단(37)은 암호관리도메인A~C마다 키관리장치와 암호장치와 통신단말의 어드레스를 기억한다.

다른구성요소는 상기 실시형태에서 기술한 구성요소와 마찬가지로 설명은 생략한다. 또, NODE형 암호장치(81)~(88)과 HUB형 암호장치(51)~(54)는 도22에서 기술한 블록도와 마찬가지로 설명은 생략한다.

암호관리도메인A에서는 키관리장치(71)이 공통 섹션키와 로컬키를 여러개 생성하고 암호관리도메인A에 속하는 암호장치(81)~(83)과 암호장치(51)로 배송한다. 또, 공통 섹션키는 키관리장치(71), (72)로 배송한다. 또, 안전강화를 위해 키관리장치(71)은 로컬키를 정기적으로 생성하고 각 암호장치의 로컬키를 갱신한다.

또, 키관리장치(71)은 암호화조건 설정수단(62)에 의해 암호장치(81)~(83)의 암호화조건 기억수단(811)~(831)에 암호화조건을 설정한다. 키관리장치(71)의 포트조건 설정수단(63)은 암호장치(51)의 포트조건 기억수

단(921)에 포트조건을 설정한다.

또, 암호관리도메인B, C에 있어서도 키관리장치(72), (73)이 마찬가지로 암호관리도메인내에서 사용하는 로컬키를 정기적으로 생성한다. 또, 공통 섹션키는 키관리장치(71)에서 배송된 것을 사용한다. 키관리장치(72), (73)이 로컬키와 공통 섹션키를 사용해서 암호화조건 및 포트조건을 소속된 암호장치에 설정한다.

다음에, 키관리장치(71)이 공통 섹션키를 생성하고 배송하는 수순을 기술한다.

우선, 암호관리도메인A와 암호관리도메인B 사이에서 키번호 5, 8, 32를 공통 섹션키로 하면 결정되어 있는 경우에 대해서 기술한다.

[1] 키관리장치(71)의섹션키 생성수단(31)이 32개의 섹션키를 생성한다.

[2] 섹션키 생성수단(31)에서 섹션키가 32개 생성되면, 섹션키 관리수단(32)는 섹션키 테이블(64)에 작성한 섹션키를 라이트한다. 섹션키 관리수단(32)는 섹션키 테이블(64)의 키번호 5, 8, 32에 대응하는 허가플래그를 「비작성」으로 한다(도면에서는 ×표). 또, 키번호 5, 8, 32에 대응하여 속성란에 암호관리도메인A와 암호관리도메인B 사이의 공통 섹션키인 것을 나타내는 “공통(A, B)”를 라이트한다.

[3] 섹션키 관리수단(32)는 암호관리도메인B에 생성한 공통키1~3을 배송하기 위해 섹션키 암호화수단(34)에서 공통키1~3을 암호화하고 섹션키 송신수단(35)에서 암호관리도메인B의 키관리장치(72)로 송신한다.

[4] 암호관리도메인B의 키관리장치(72)에 있어서의 섹션키 수신수단(65)는 키관리장치(71)의 섹션키 송신수단(35)에서 송신되고 암호화된 섹션키를 수신한다. 키관리장치(72)에 있어서의 섹션키 관리수단(32)는 수신되고 암호화된 공통 섹션키를 복호수단(66)에 전달한다. 섹션키 복호수단(66)은 암호화된 공통 섹션키를 복호한다. 키관리장치(72)에 있어서의 섹션키 관리수단(32)는 복호된 공통 섹션키를 섹션키 테이블(64)의 키번호 5, 8, 32에 대응하는 키란에 라이트하고, 허가플래그를 「비작성」으로 한다. 또, 섹션키 테이블(64)의 키번호 5, 8, 32에 대응하는 속성란에 암호관리도메인A와 암호관리도메인B 사이의 공통 섹션키인 것을 나타내는 “공통(A, B)”를 라이트한다. 키관리장치(72)의 섹션키 테이블(64)에 있어서 키번호 5, 8, 32에 이미 공통 섹션키가 라이트되어 있는 경우에는 오버라이트된다.

[5] 키관리장치(72)의 섹션키 생성수단(31)은 자기 암호관리도메인을 위한 로컬키를 생성한다. 섹션키 관리수단(32)는 섹션키 테이블(64)의 허가플래그가 「작성」(도면에서는 ○표)로 되어 있는 키번호에 섹션키 생성수단(31)이 생성한 섹션키를 로컬키로서 라이트한다.

키관리장치(71), (72)의 로컬키는 상기 실시형태에서 기술한 것과 동일 방법으로 자기 암호관리도메인의 암호장치로 배송된다.

다음에, 키관리장치(71)이 공통 섹션키를 생성하고 배송하는 다른 수순에 대해서 기술한다.

암호관리도메인A, B, C에서 암호통신하기 위한 공통 섹션키를 공통키1로 한다. 암호관리도메인A, B가 암호통신하기 위한 공통 섹션키를 공통키2로 한다. 암호관리도메인A, C가 암호통신하기 위한 공통 섹션키를 공통키3으로 한다. 암호관리도메인B, C가 암호통신하기 위한 공통 섹션키를 공통키4로 한다. 이 경우, 키관리장치(71)이 공통키1~4를 생성하고, 암호관리도메인B의 키관리장치(72)로 공통키1, 2, 4를 배송한다. 암호관리도메인C의 키관리장치(73)으로는 공통키1, 3, 4를 배송한다.

처음에 기술한 방법에서는 키관리장치(71)과 (72) 사이에서 키번호5, 8, 32를 공통 섹션키를 등록하는 키번호로 정하고 있었다. 그러나, 예를 들면 키관리장치(71)이 생성한 32개의 섹션키중에서 임의로 4개의 공통키1~4를 선택해내어 해당하는 허가플래그를 「비작성」으로 한다. 키관리장치(71)은 섹션키 테이블(64)의 속성란에 어느 암호관리도메인 사이의 공통 섹션키로 할지를 라이트한다. 또, 키관리장치(71)은 해당하는 키관리장치로 공통 섹션키와 속성정보를 배송한다. 배송된 키관리장치에서는 섹션키 테이블(64)에 있어서의 공통섹

션키를 기억하고 있던 임의의 키번호의 위치에 공통 색션키를 라이트하고, 허가플래그를 「비작성」으로 하여 속성에 어떠한 암호관리도메인과의 공통 색션키인지를 라이트한다. 이와 같은 방법으로 각 암호관리도메인에 공통 색션키를 배속관리해도 좋다.

암호관리도메인B, C에서 각각 필요로 하는 공통키1~4를 배속한 후, 각 키관리장치(71)~(73)은 상기 실시형태3에서 기술한 바와 같이 자기 암호관리도메인내의 암호장치에 대해 암호화조건 설정수단(62)와 포트조건 설정수단(63)을 사용해서 암호화조건과 포트조건을 설정한다. 암호화조건과 포트조건에 있어서의 기본패스와 특예패스의 설정에 대해서는 상기 실시형태와 마찬가지로 설명은 생략한다.

도37에 공통키1~4를 사용해서 암호화조건과 포트조건을 설정한 경우 형성되는 암호관리도메인을 초과한 논리그룹의 예를 도시한다.

통신단말(2c), (2d), (2h), (2k)가 공통키1에 의해 암호화/복호되는 암호통신을 실행하는 논리그룹1을 형성한다. 통신단말(2a), (2b), (2f)가 공통키2에 의해 암호화/복호되는 암호통신을 실행하는 논리그룹2를 형성한다. 통신단말(2d), (2i), (2m)이 공통키3에 의해 암호화/복호되는 암호통신을 실행하는 논리그룹3을 형성한다. 통신단말(2e), (2f), (2j), (2k)는 공통키4에 의해 암호화/복호되는 암호통신을 실행하는 논리그룹4를 형성한다. 이와 같이 각각 독자의 색션키를 갖는 암호관리도메인 사이에서 공통 색션키를 공유하는 것에 의해 암호관리도메인의 벽을 넘은 새로운 논리그룹이 통신단말 사이에서 형성된다.

이상과 같이 이 실시형태에서는 키관리장치와 암호장치와 통신단말로 이루어지는 암호관리도메인이 여러개 있고, 각 암호관리도메인은 키관리장치가 암호관리도메인내의 로컬키를 생성하고 관리한다. 이들 암호관리도메인 사이에서 암호통신을 실행하기 위한 공통 색션키를 공유하고 또한 암호조건과 포트조건을 공통 색션키를 사용해서 설정하는 것에 의해 다른 암호관리도메인에 속하는 통신단말끼리가 공통 색션키에 의해 암호화된 암호통신을 실행할 수 있다. 또, 기본패스 및 특예패스의 설정에 있어서, 수신지 IP어드레스, 어플리케이션, 통신방향, 색션키를 설정하는 것이 가능하므로, 다른 암호관리도메인 사이의 통신단말 사이에서 논리그룹을 형성할 수 있다. 또, 수신지 IP어드레스, 어플리케이션, 통신방향에서 공통 색션키에 의한 암호통신을 설정하는 것이 가능하므로 사용자측의 편리성과 함께 안전의 향상을 도모할 수 있다.

발명의 효과

이상과 같이 본 발명에 의하면, 그룹화된 여러개의 통신단말 사이에서 통신데이터를 암호화 또는 복호할 수 있다.

또, 본 발명에 의하면, 모드스위치의 설정에 의해 암호통신과 평문통신 중 어느 하나를 선택할 수 있다.

또, 본 발명에 의하면, 암호장치마다 통신데이터의 암호화조건을 설정할 수 있어 암호화조건에 의해 통신데이터를 암호화할지 하지 않을지를 판정할 수 있다.

또, 본 발명에 의하면, 키관리장치에 있어서 그룹마다 개별의 색션키를 생성할 수 있다.

또, 본 발명에 의하면, 암호장치에서 설정된 모드스위치를 유효로 할지 무효로 할지를 키관리장치에서 관리할 수 있다.

또, 본 발명에 의하면, 여러개의 암호관리도메인끼리에서 암호통신을 실행할 수 있다.

⑤7 특허청구의 범위

1. 그룹화된 여러개의 통신장치와 적어도 상기 여러개의 통신장치의 1개 이상의, 통신장치에 대응해서 각각 마련된 여러개의 암호장치로서, 상기 그룹에 속하는 통신장치가 송수신하는 통신데이터를 암호화 또는 복호하

는 섹션키를 적어도 1개 기억하는 섹션키 기억수단, 상기 섹션키에 의해 통신데이터를 암호화 또는 복호하는 암호처리수단 및 상기 암호처리수단에 의해 처리된 통신데이터를 송수신하는 데이터 송수신수단을 구비한 여러개의 암호장치를 구비하는 것을 특징으로 하는 암호화시스템.

2. 그룹화된 여러개의 통신장치와 적어도 상기 여러개의 통신장치의 1개 이상의 통신장치에 대응해서 각각 마련된 여러개의 암호장치로서, 상기 그룹에 속하는 통신장치가 송수신하는 통신데이터를 암호화 또는 복호하는 섹션키를 적어도 1개 기억하는 섹션키 기억수단, 상기 섹션키에 의해 통신데이터를 암호화 또는 복호하는 암호처리수단, 상기 암호처리수단에 의해 처리된 통신데이터를 송수신하는 데이터 송수신수단 및 상기 섹션키 기억수단에 섹션키를 적어도 1개 기억시키고, 상기 섹션키에 의해 통신데이터를 암호화 또는 복호할지 복호하지 않을지를 설정하는 모드스위치를 구비한 여러개의 암호장치를 구비하는 것을 특징으로 하는 암호화시스템.

3. 그룹화된 여러개의 통신장치와 적어도 상기 여러개의 통신장치의 1개 이상의 통신장치에 대응해서 각각 마련된 여러개의 암호장치로서, 상기 그룹에 속하는 통신장치가 송수신하는 통신데이터를 암호화 또는 복호하는 섹션키를 적어도 1개 기억하는 섹션키 기억수단, 상기 섹션키에 의해 통신데이터를 암호화 또는 복호하는 암호처리수단, 상기 암호처리수단에 의해 처리된 통신데이터를 송수신하는 데이터 송수신수단, 통신데이터의 암호화에 관한 암호화조건을 기억하는 암호화조건 기억수단, 및 상기 암호화조건에 따라서 통신데이터를 암호화 또는 복호할지 복호하지 않을지를 판정하는 조건판정수단을 구비한 여러개의 암호장치를 구비하는 것을 특징으로 하는 암호화시스템.

4. 그룹화된 여러개의 통신장치와 적어도 상기 여러개의 통신장치의 1개 이상의 통신장치에 대응해서 각각 마련된 여러개의 암호장치로서, 상기 그룹에 속하는 통신장치가 송수신하는 통신데이터를 암호화 또는 복호하는 섹션키를 적어도 1개 기억하는 섹션키 기억수단, 상기 섹션키에 의해 통신데이터를 암호화 또는 복호하는 암호처리수단, 상기 암호처리수단에 의해 처리된 통신데이터를 송수신하는 데이터 송수신수단, 통신데이터의 암호화에 관한 암호화조건을 기억하는 암호화조건 기억수단 및 상기 암호화조건에 따라서 통신데이터를 암호화 또는 복호할지 복호하지 않을지를 판정하는 조건판정수단을 구비한 여러개의 암호장치를 구비하고, 그룹화된 통신장치를 기억하는 통신장치 그룹기억수단과 상기 통신장치 그룹 기억수단에 의해 기억된 그룹마다 개별의 섹션키를 생성해서 출력하는 섹션키 생성수단을 더 구비한 관리장치를 구비하는 것을 특징으로 하는 암호화시스템.

5. 그룹화된 여러개의 통신장치와 적어도 상기 여러개의 통신장치의 1개 이상의 통신장치에 대응해서 각각 마련된 여러개의 암호장치로서, 상기 그룹에 속하는 통신장치가 송수신하는 통신데이터를 암호화 또는 복호하는 섹션키를 적어도 1개 기억하는 섹션키 기억수단, 상기 섹션키에 의해 통신데이터를 암호화 또는 복호하는 암호처리수단, 상기 암호처리수단에 의해 처리된 통신데이터를 송수신하는 데이터 송수신수단, 상기 섹션키 기억수단에 섹션키를 적어도 1개 기억하고, 상기 섹션키에 의해 통신데이터를 암호화 또는 복호할지 복호하지 않을지를 설정하는 모드스위치 및 상기 모드스위치의 설정과 송신된 상기 유효무효정보에서 통신데이터를 암호화 또는 복호할지를 판정하는 유효무효 판정수단을 구비한 여러개의 암호장치를 구비하고, 그룹화된 통신장치를 기억하는 통신장치그룹 기억수단, 상기 통신장치 그룹 기억수단에 의해 기억된 그룹마다 개별의 섹션키를 생성해서 출력하는 섹션키 생성수단 및 상기 암호장치에 구비된 상기 모드스위치의 전환을 유효로 할지 무효로 할지를 나타내는 유효무효정보를 암호장치마다 설정하고 유효무효정보를 대응하는 암호장치로 송신하는 유효무효 설정수단을 구비한 관리장치를 더 구비하는 것을 특징으로 하는 암호화시스템.

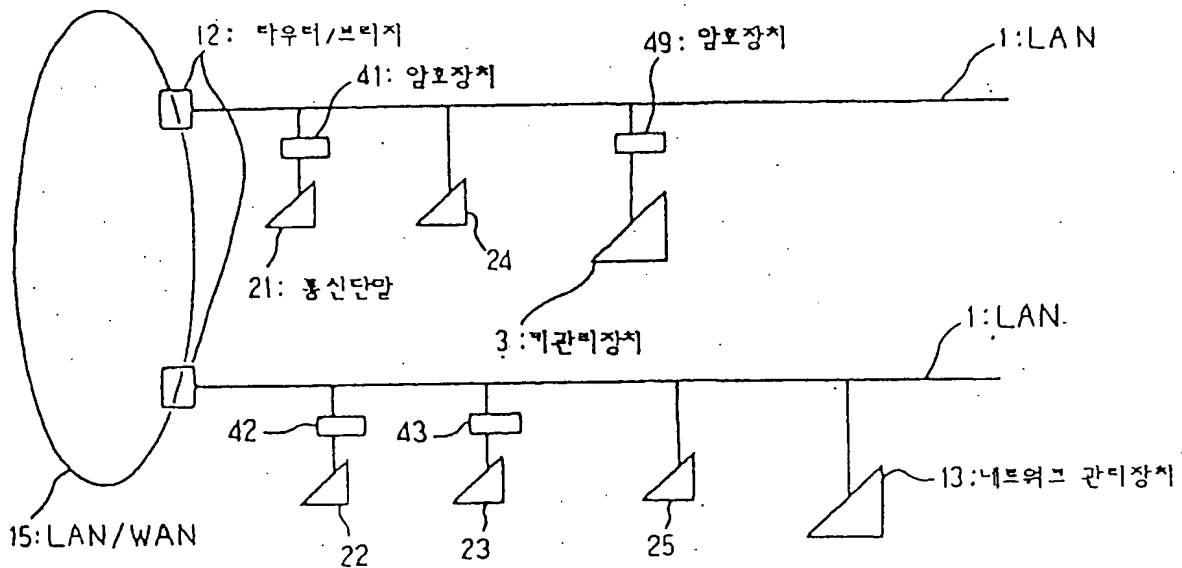
6. 여러개의 관리장치를 구비하고, 각 관리장치와 1이상의 암호장치와 1이상의 통신장치로 이루어지는

암호관리도메인을 형성하는 암호화시스템에 있어서, 상기 여러개의 관리장치는 각각의 암호관리도메인에서 사용하는 섹션키를 생성하는 섹션키 생성수단을 구비하고, 상기 여러개의 관리장치중의 1대의 관리장치에 있어서의 섹션키 생성수단은 또, 여러개의 암호관리도메인끼리의 암호통신에 있어서 사용되는 공통 섹션키를 다른 관리장치를 위해 생성하는 것을 특징으로 하는 암호화시스템.

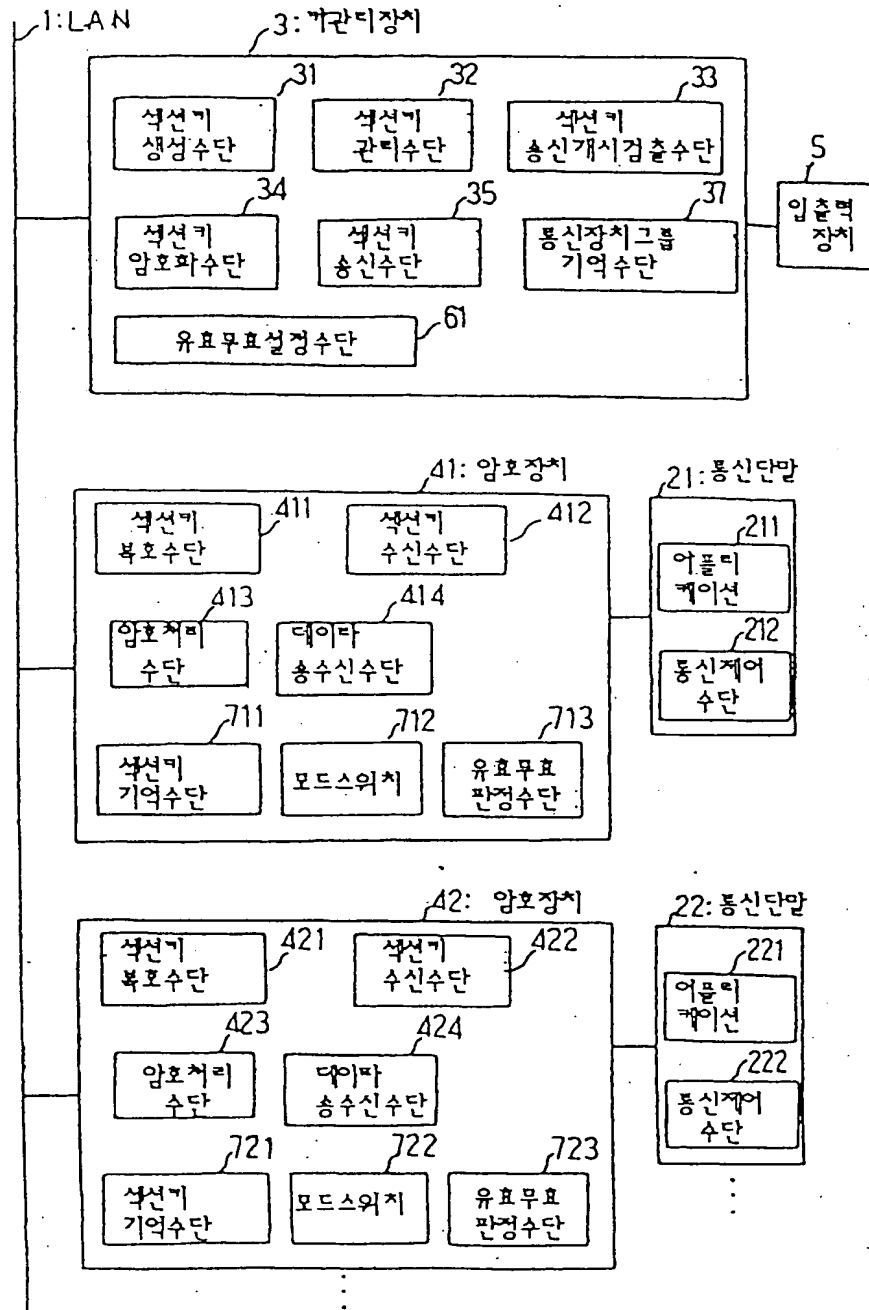
※ 참고사항 : 최초출원 내용에 의하여 공개하는 것임.

【도면】

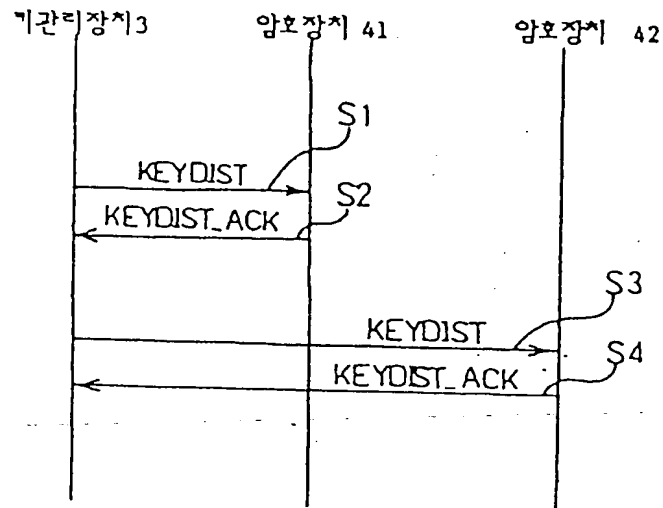
【도 1】



【도 2】



【도 3】

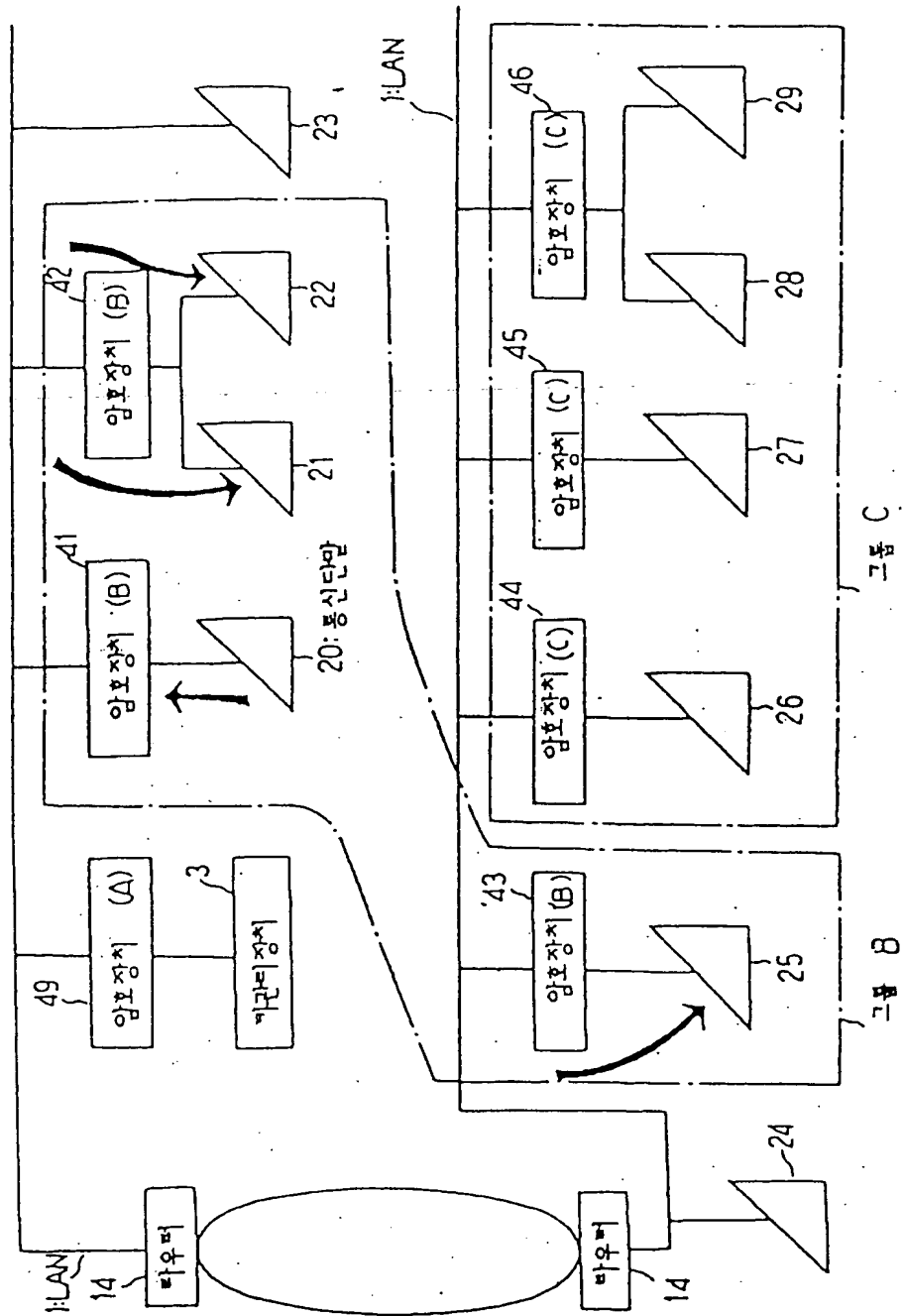


【도 5】

그룹명칭	GN	IP어드레스	비 고	유효 / 무효
기관리장치	A	aaa.aaa.aaa.aaa	관리실	무효
인사부	B	aaa.aaa.aaa.bbb	인사 1 G	유효
인사부	B	aaa.aaa.aaa.ccc	인사 1 G	무효
인사부	B	aaa.aaa.aaa.ddd	인사 2 G	무효
경리부	C	aaa.aaa.aaa.eee	경리 1 G	무효
경리부	C	aaa.aaa.aaa.fff	경리 2 G	무효
경리부	C	aaa.aaa.aaa.ggg	경리 3 G	유효

입력필드

【도 4】



【도 6】

3 1

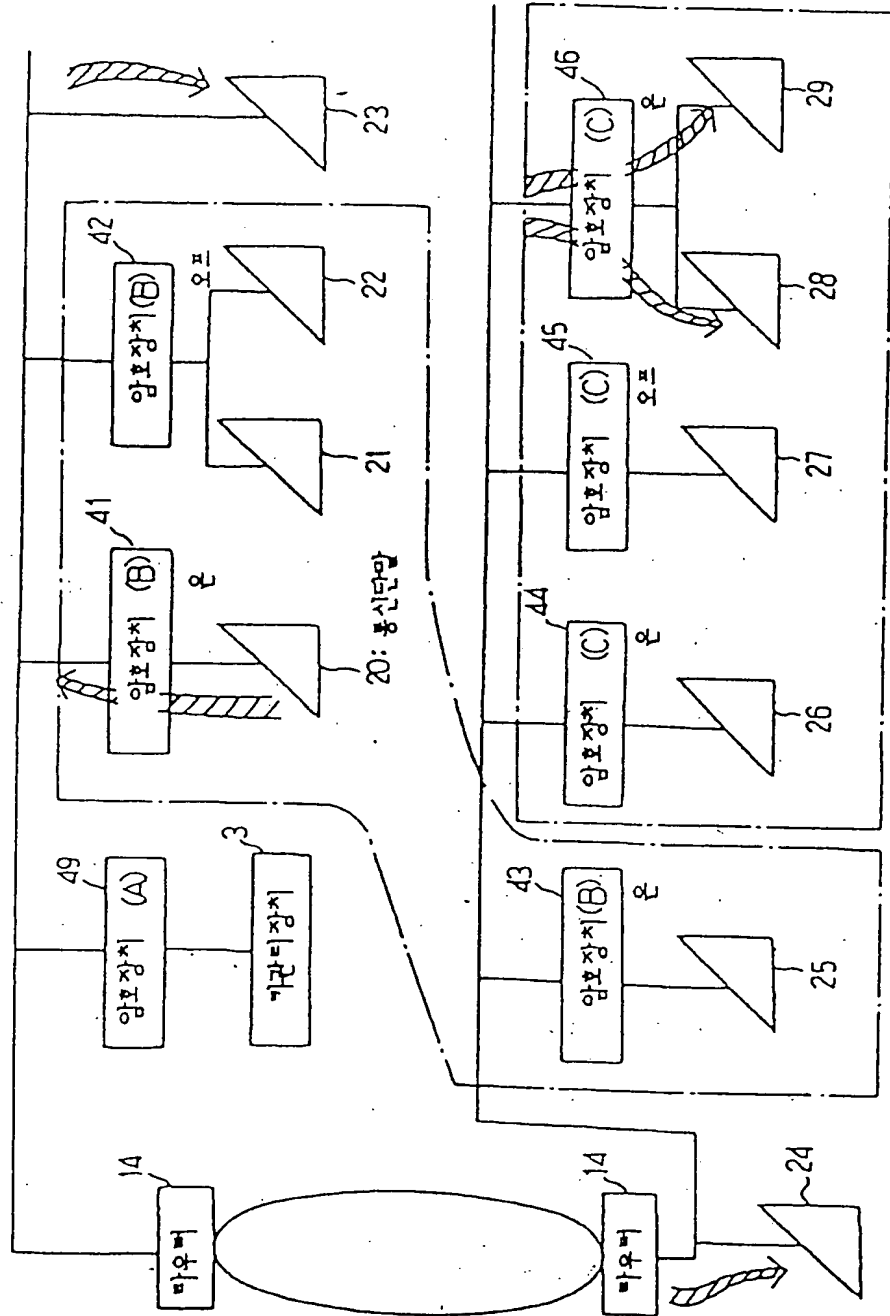
0

프로토타입		
색선키		
}}		
인증용데이터		유효/무효

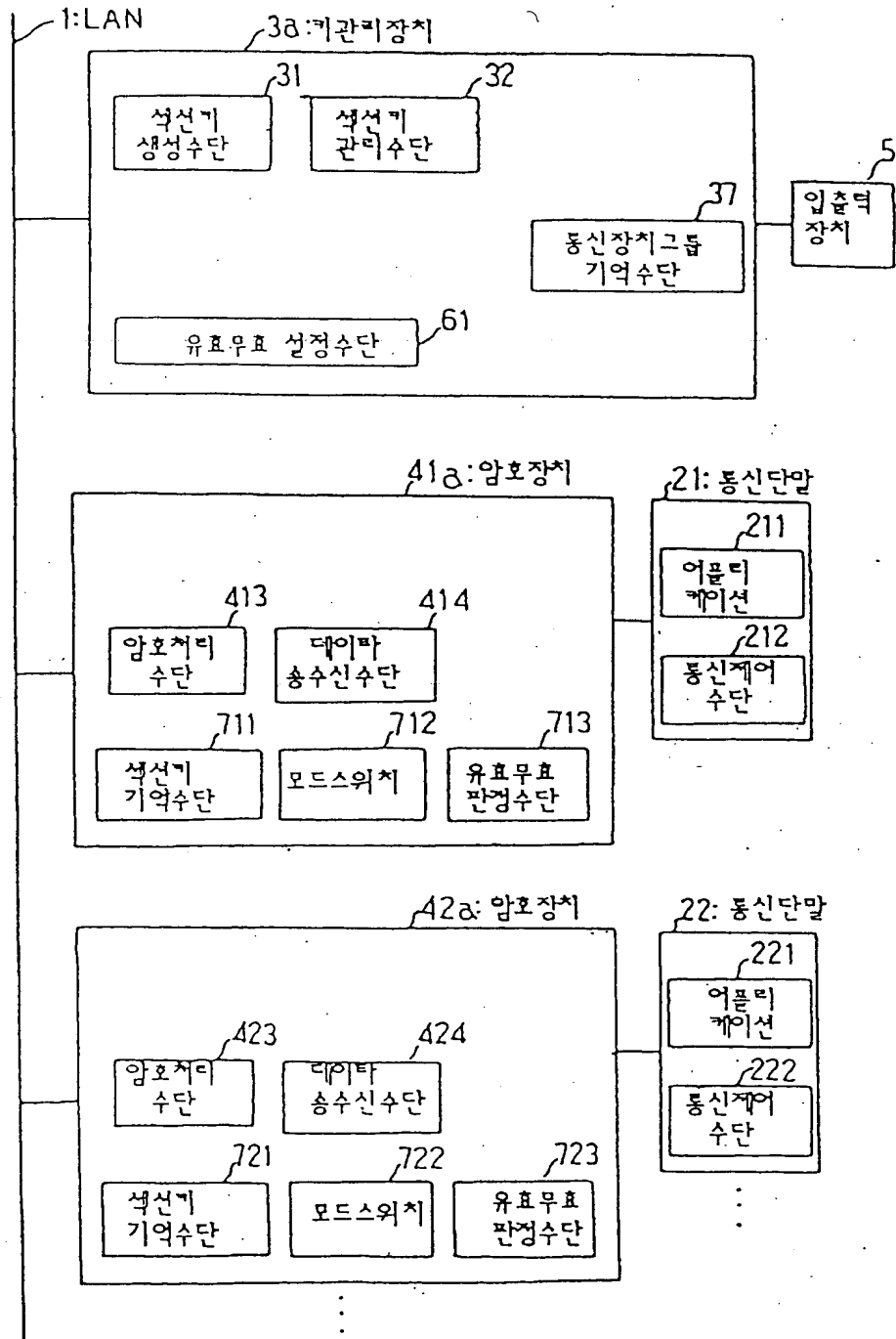
【도 7】

모드스위치	유효	무효
	유효 (1)	무효 (0)
오프 (0)	암호 (0)	암호 (0)
온 (1)	투과 (1)	암호 (0)

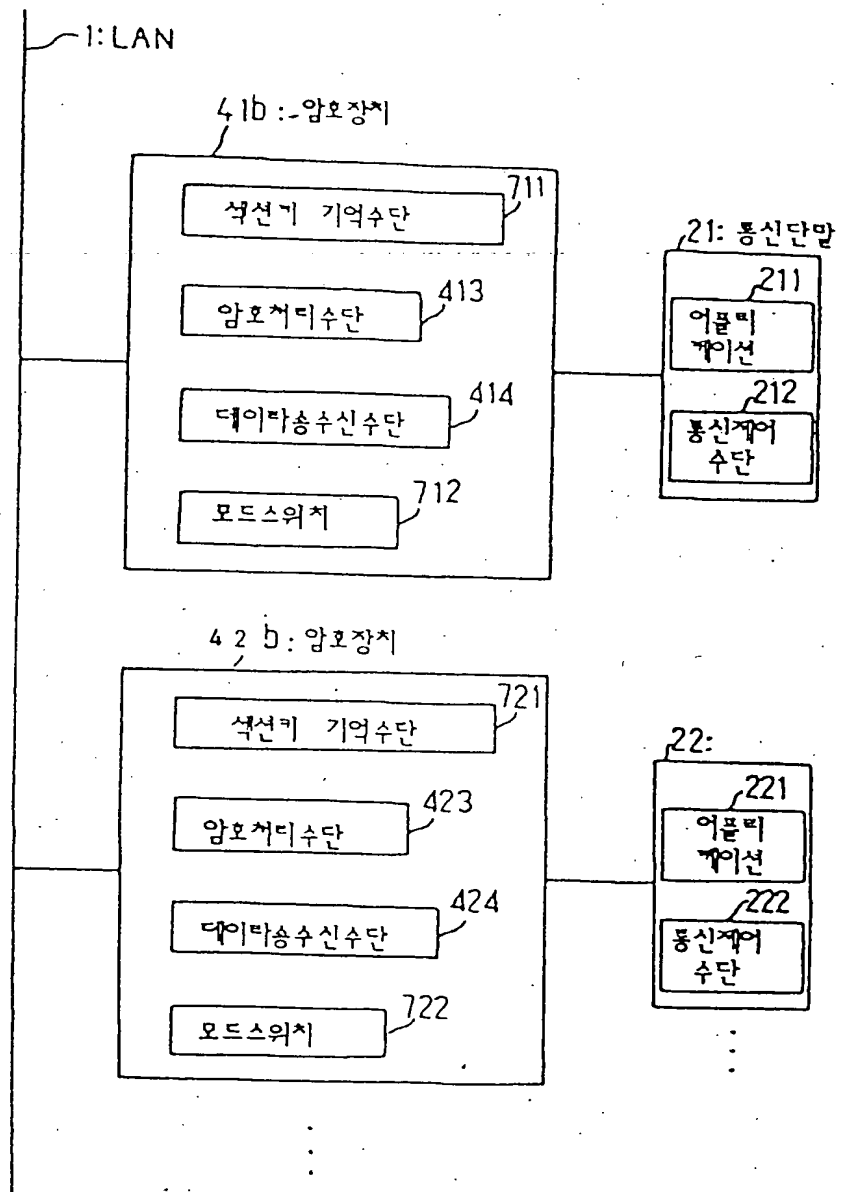
【도 8】



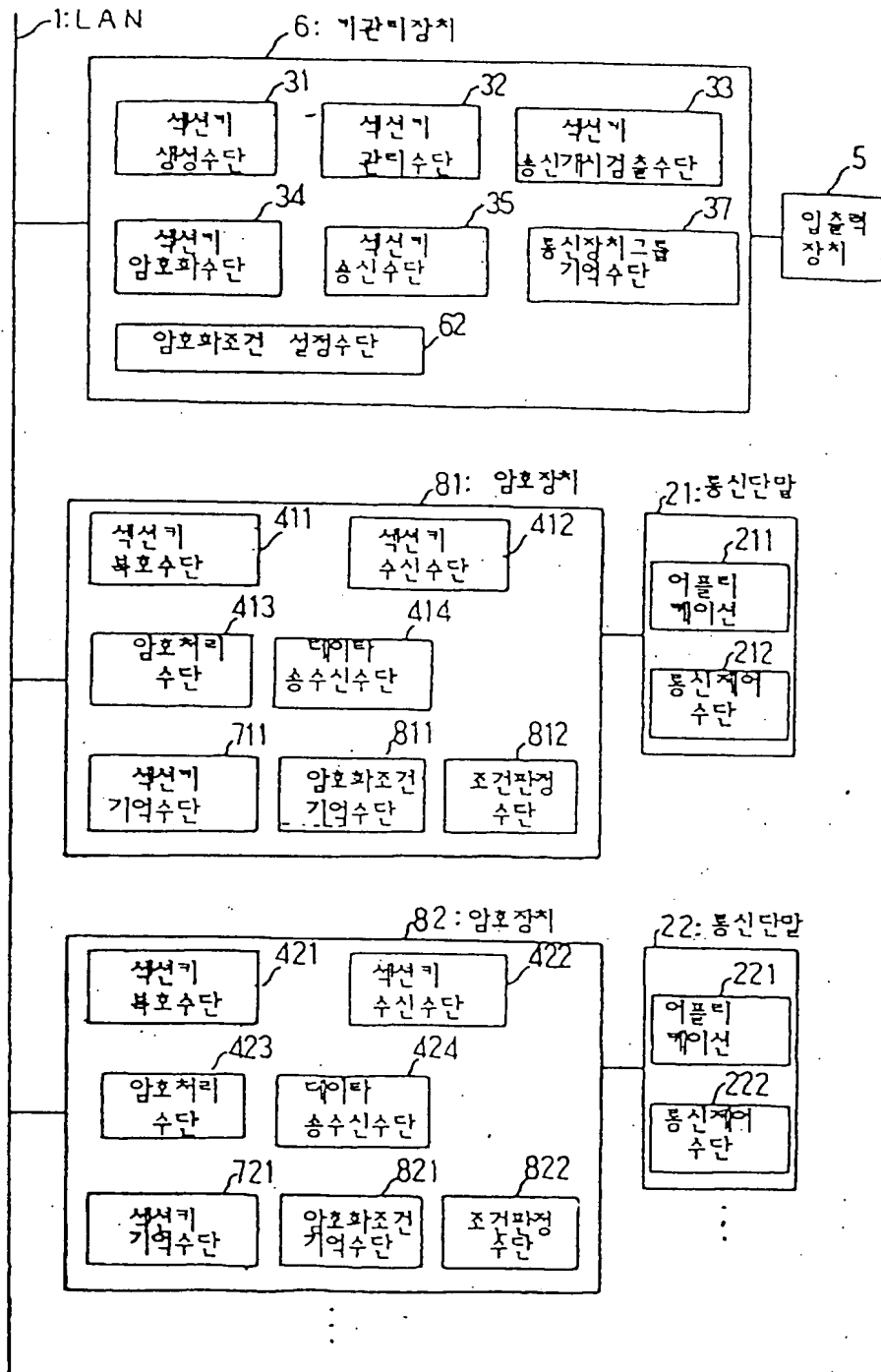
【도 9】



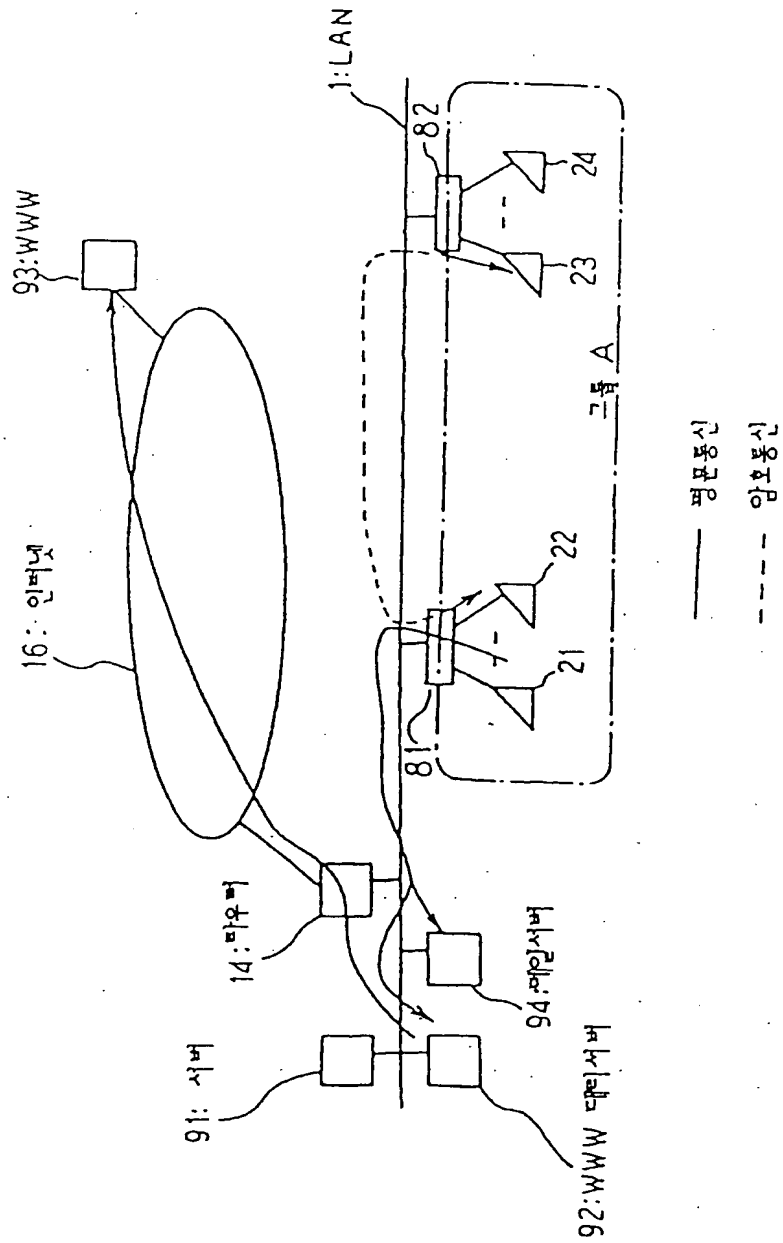
【도 10】



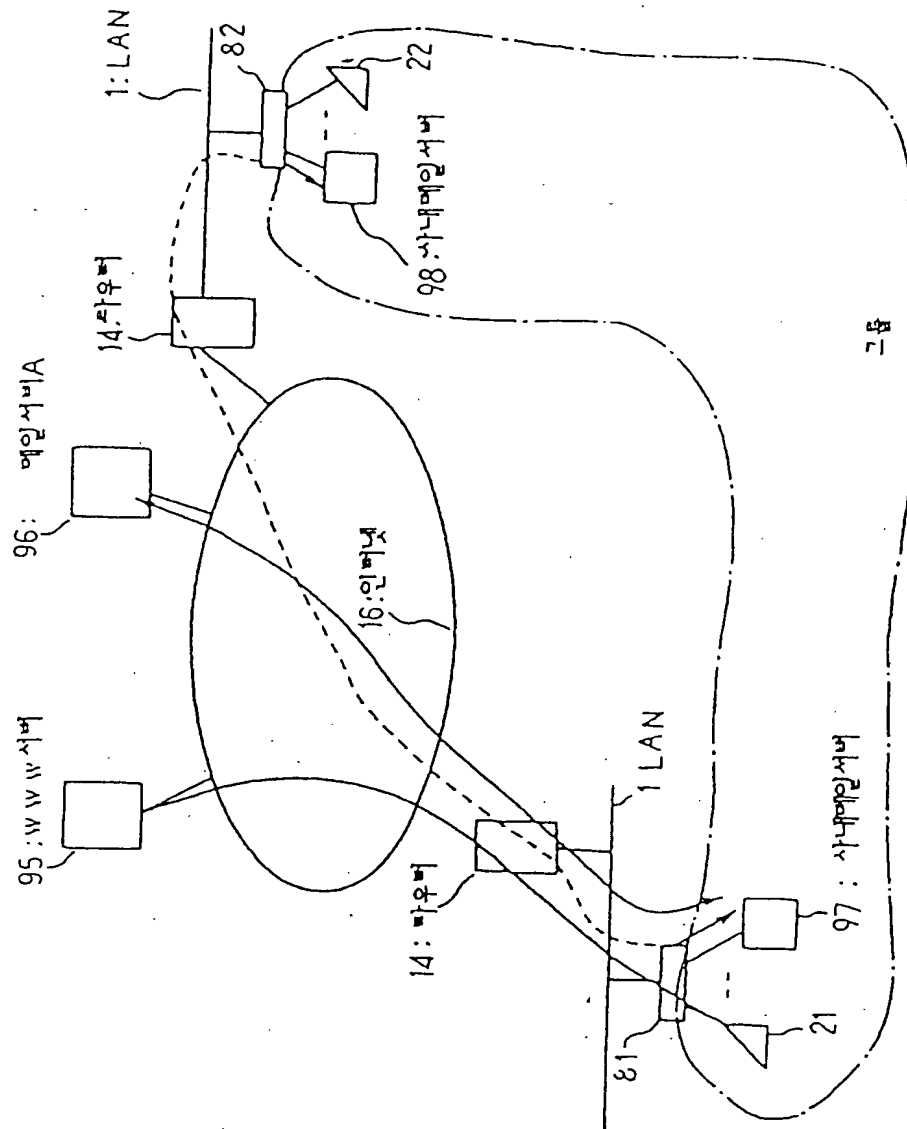
【도 11】



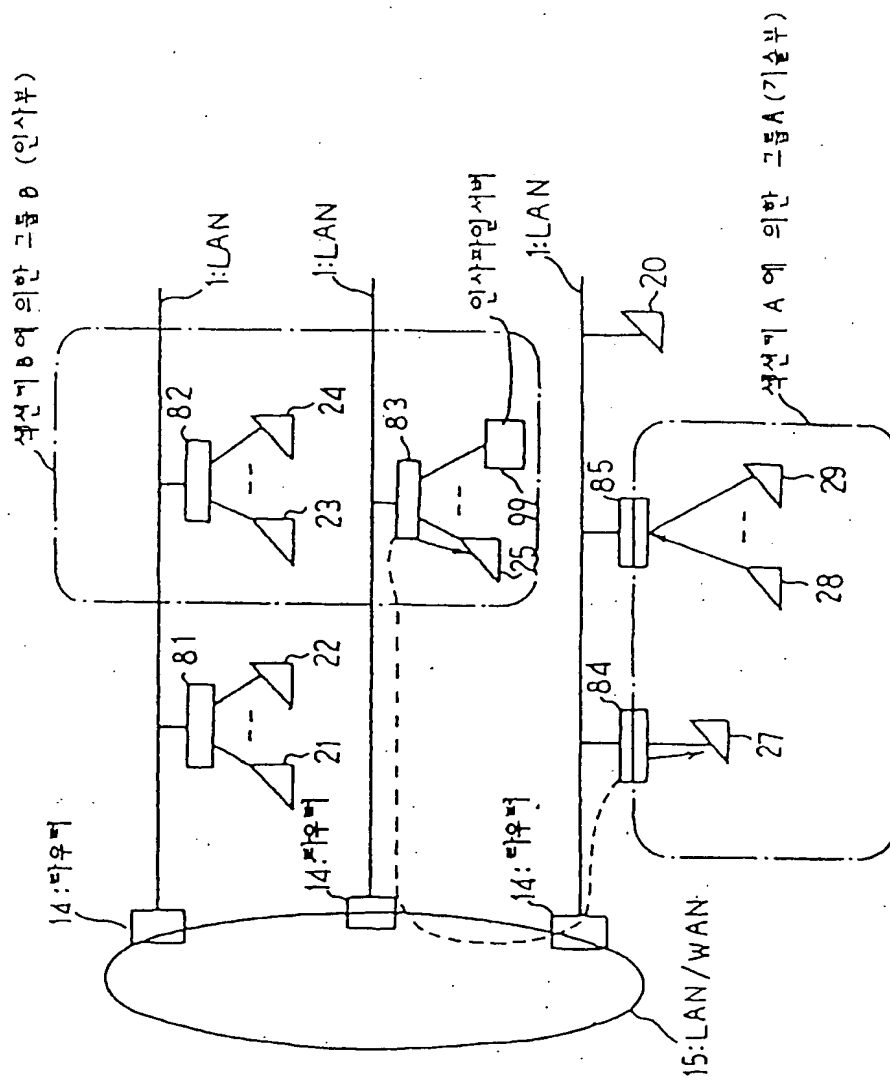
【도 12】



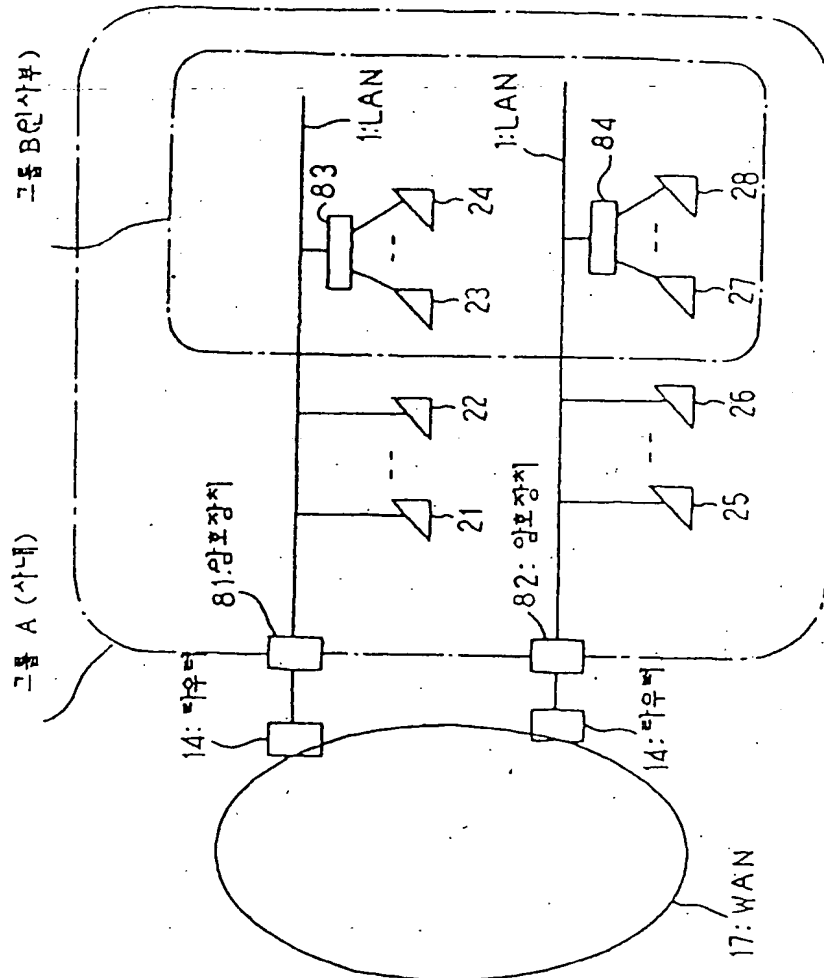
【도 13】



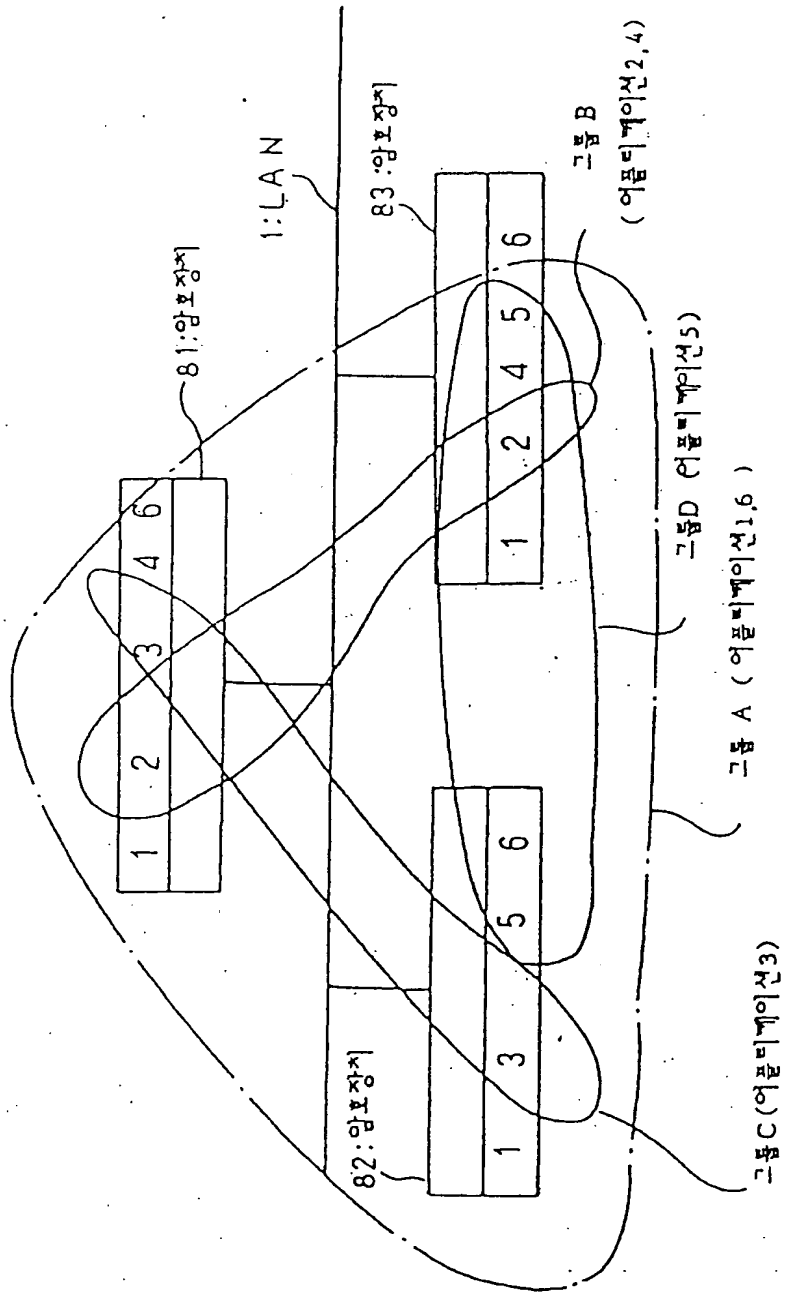
【도 14】



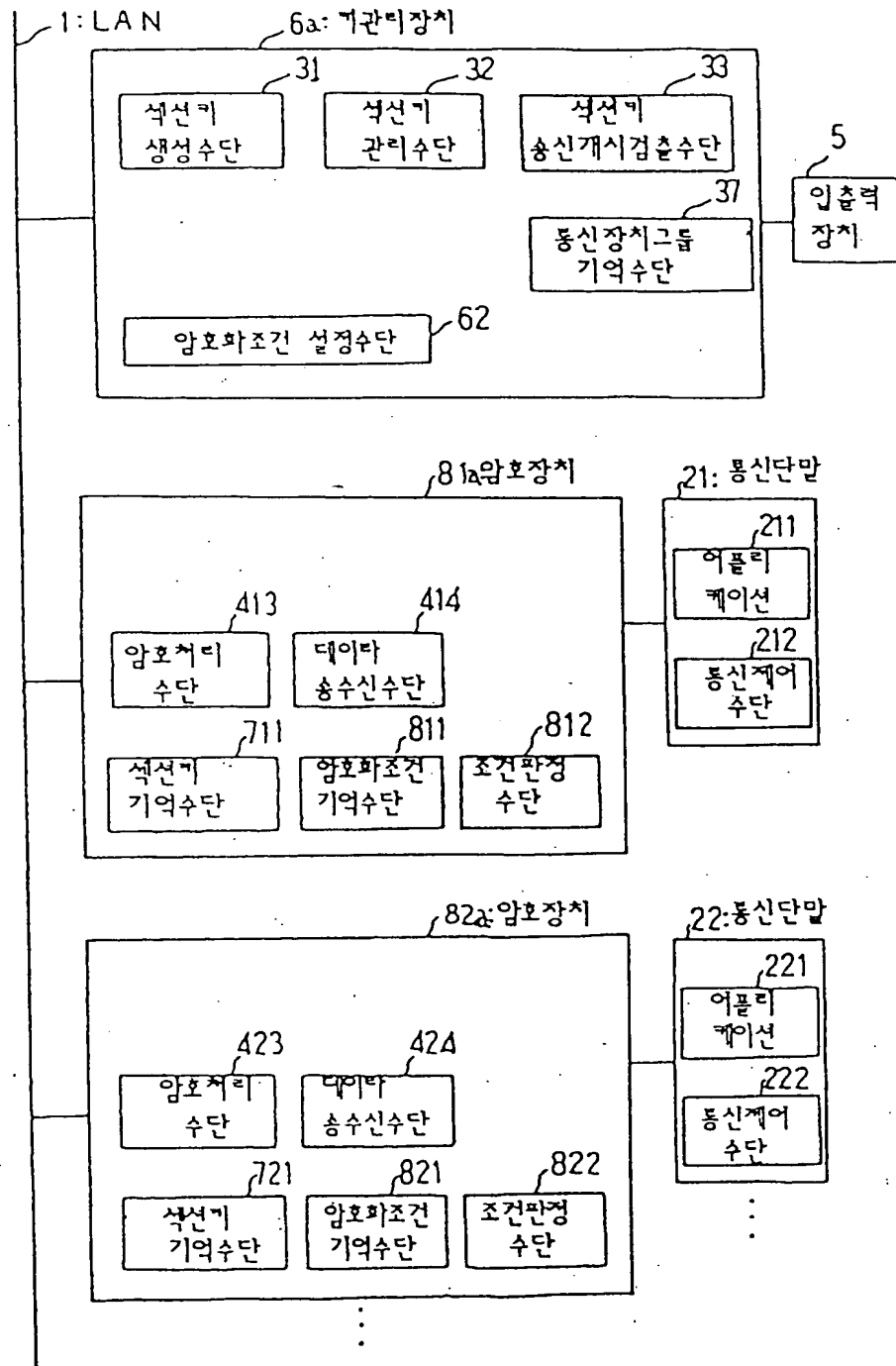
【도 15】



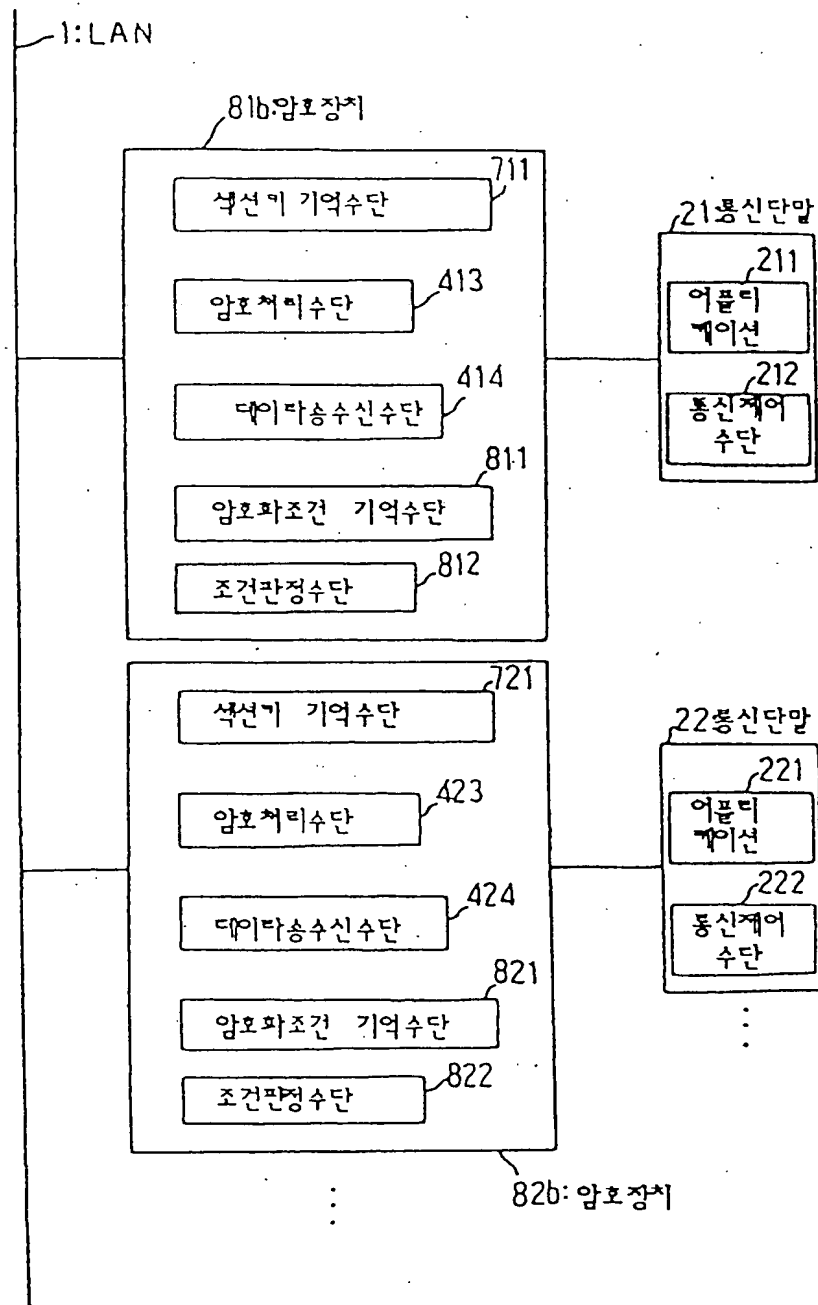
【도 16】



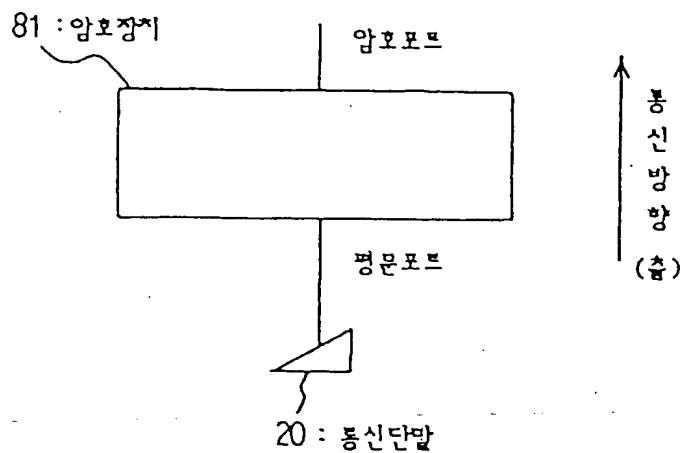
【도 17】



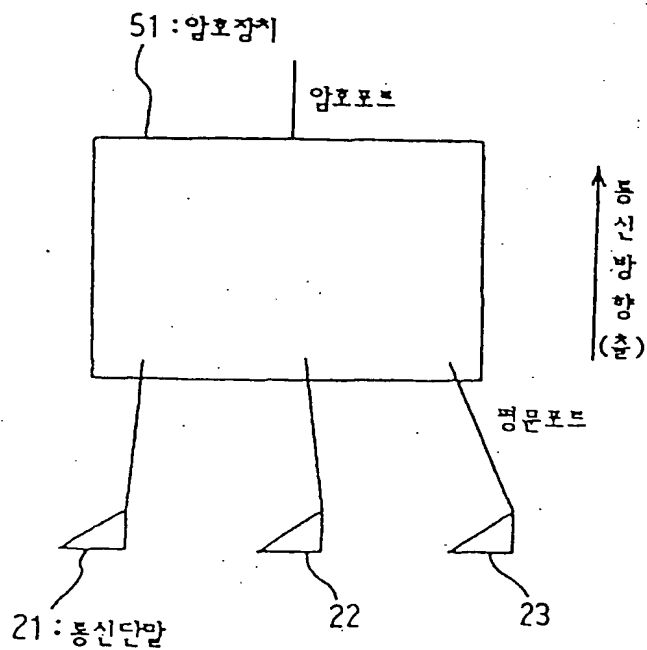
【도 18】



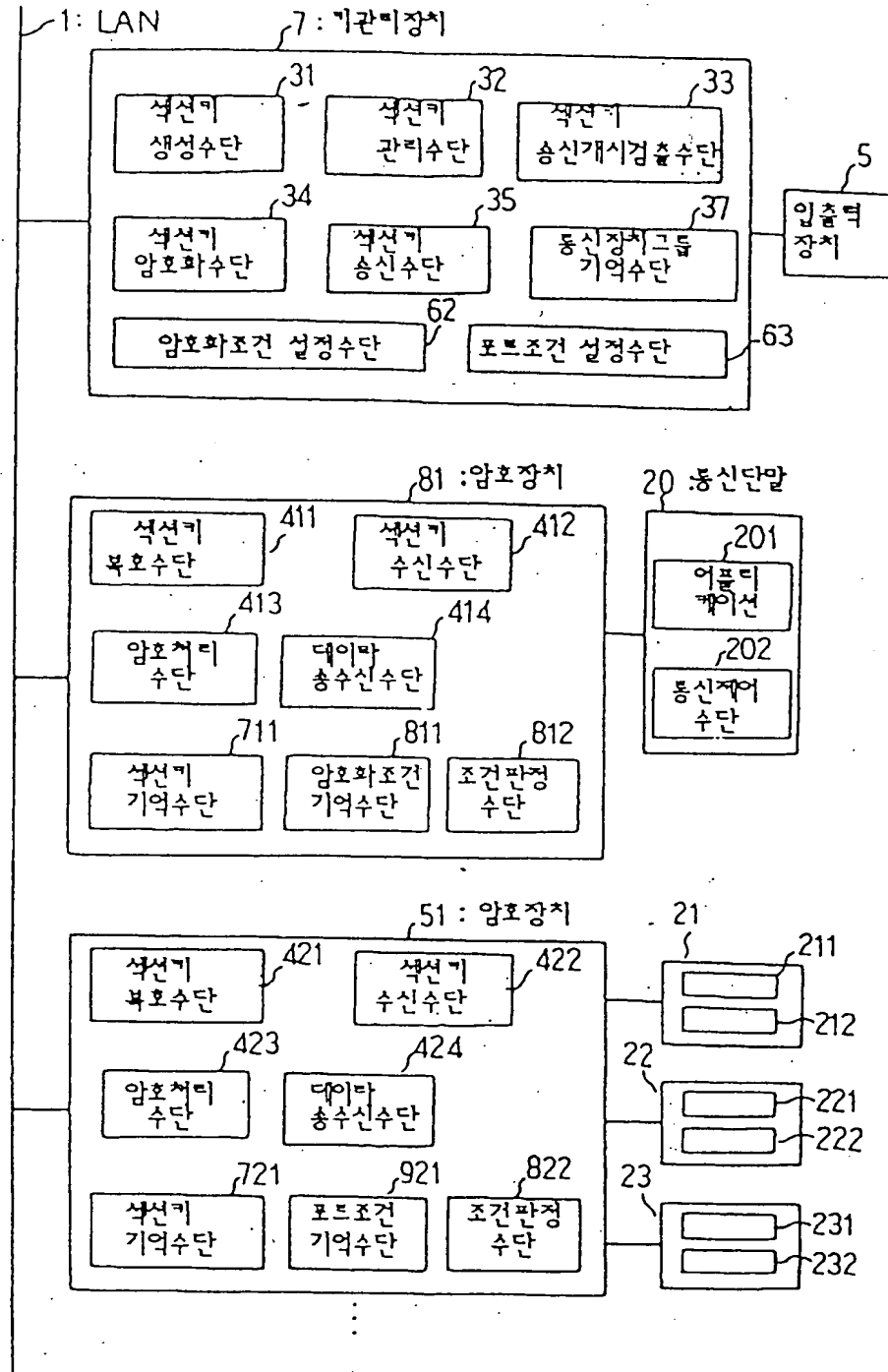
【도 20】



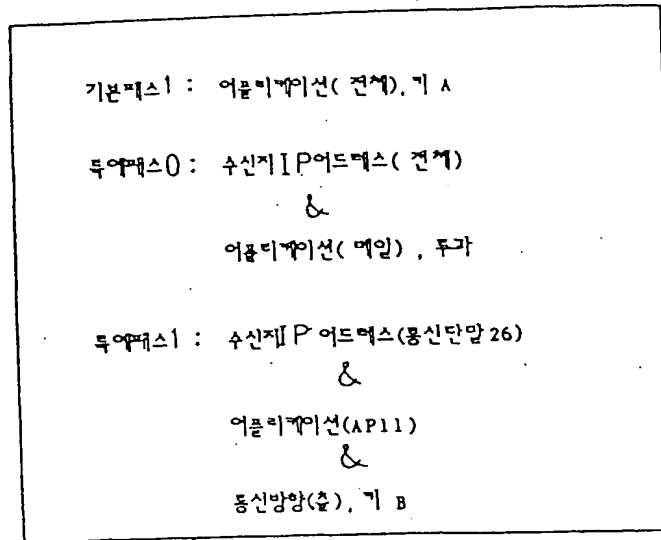
【도 21】



【도 22】

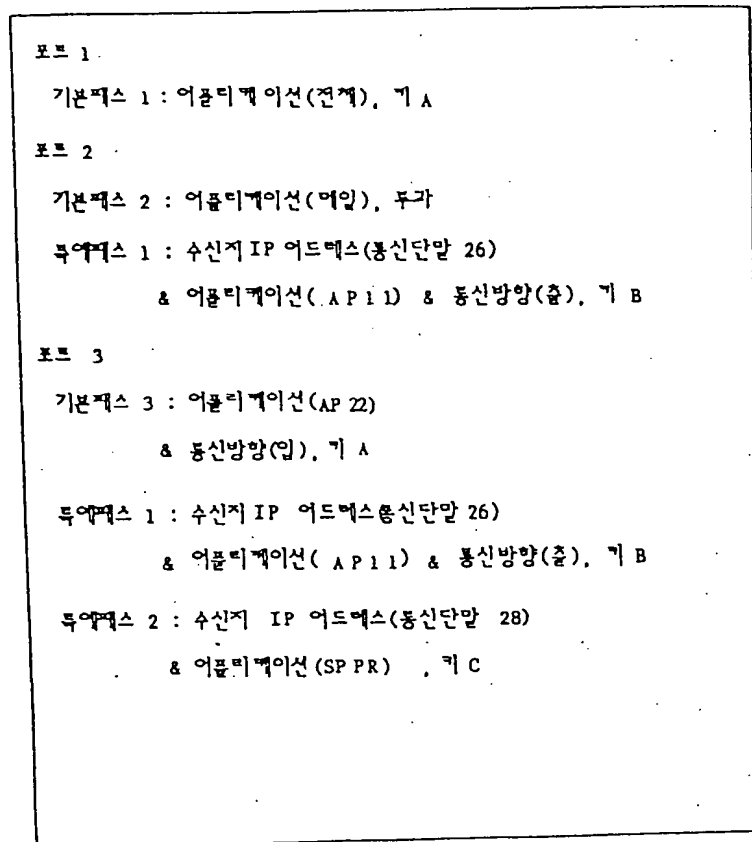


【도 23】



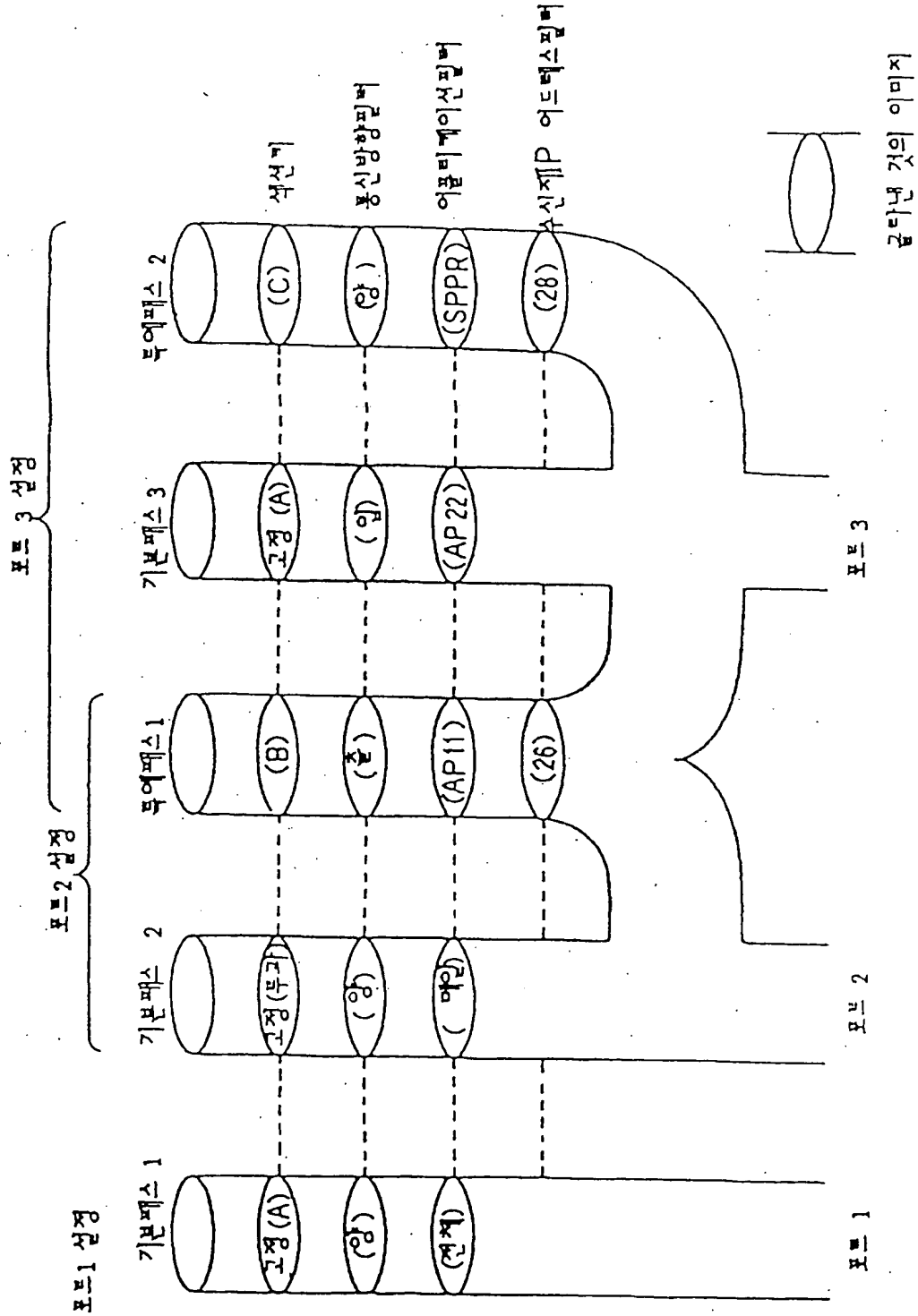
811 : 암호화조건 기억수단

【도 24】

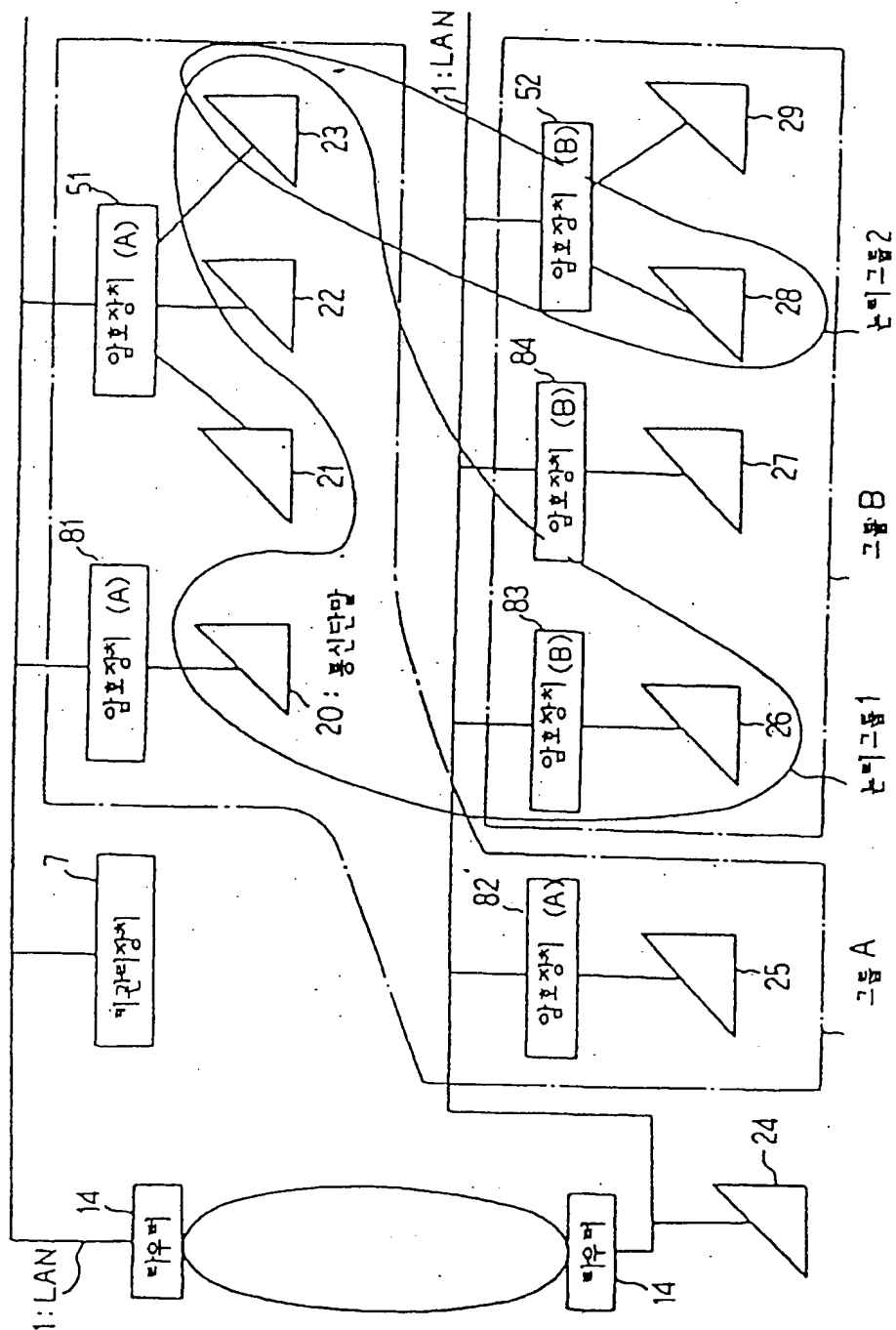


921 : 포트조건 기억수단

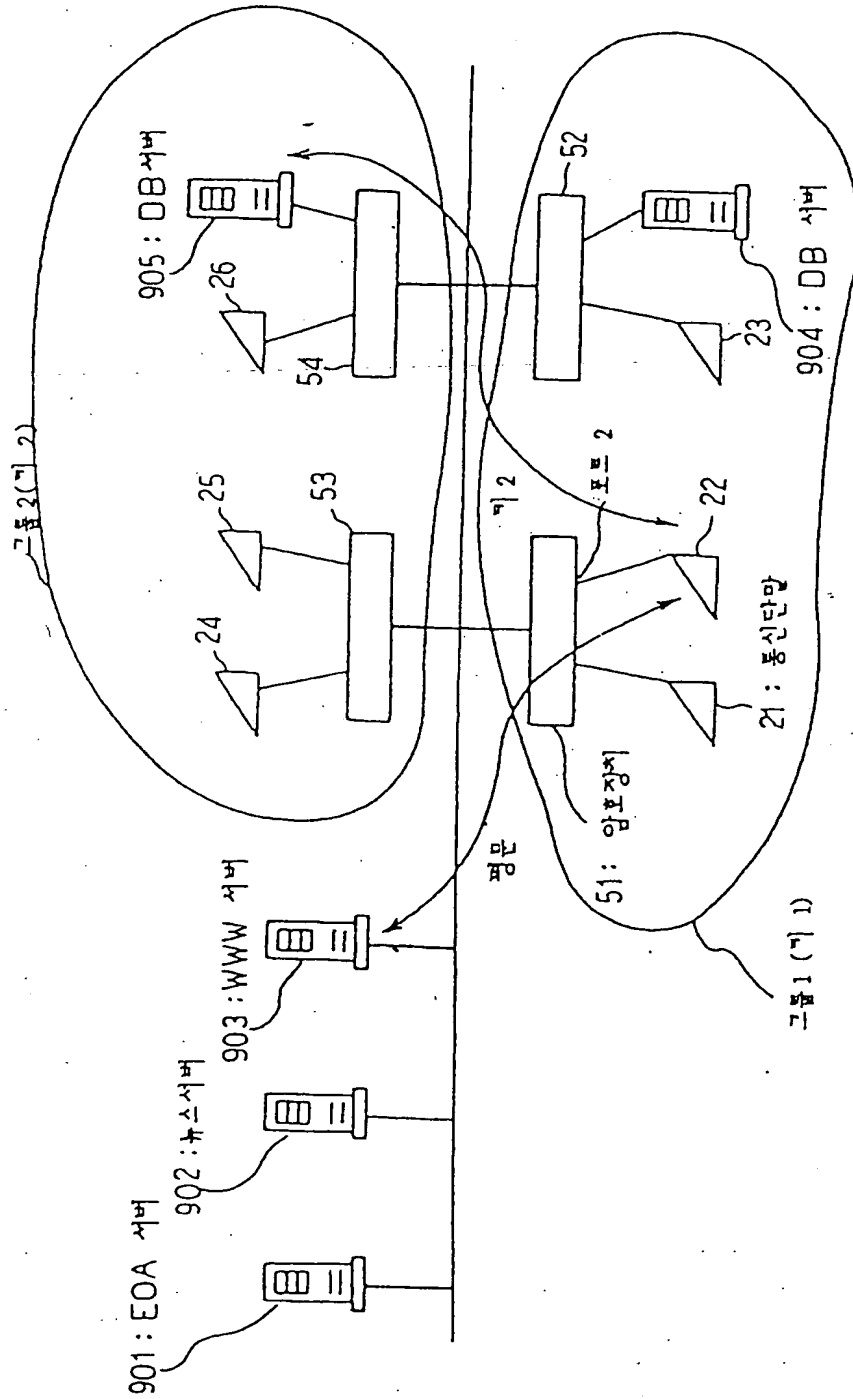
【도 25】



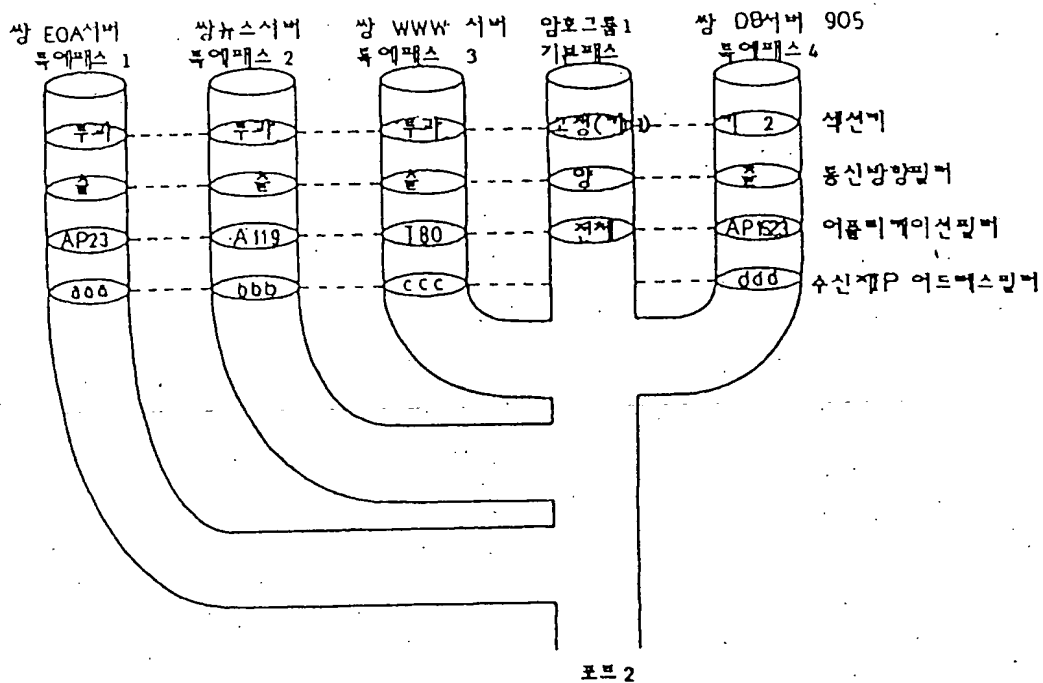
【도 26】



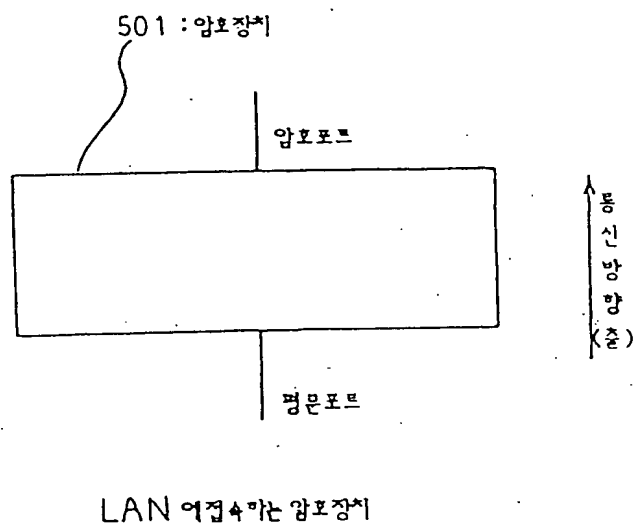
【도 27】



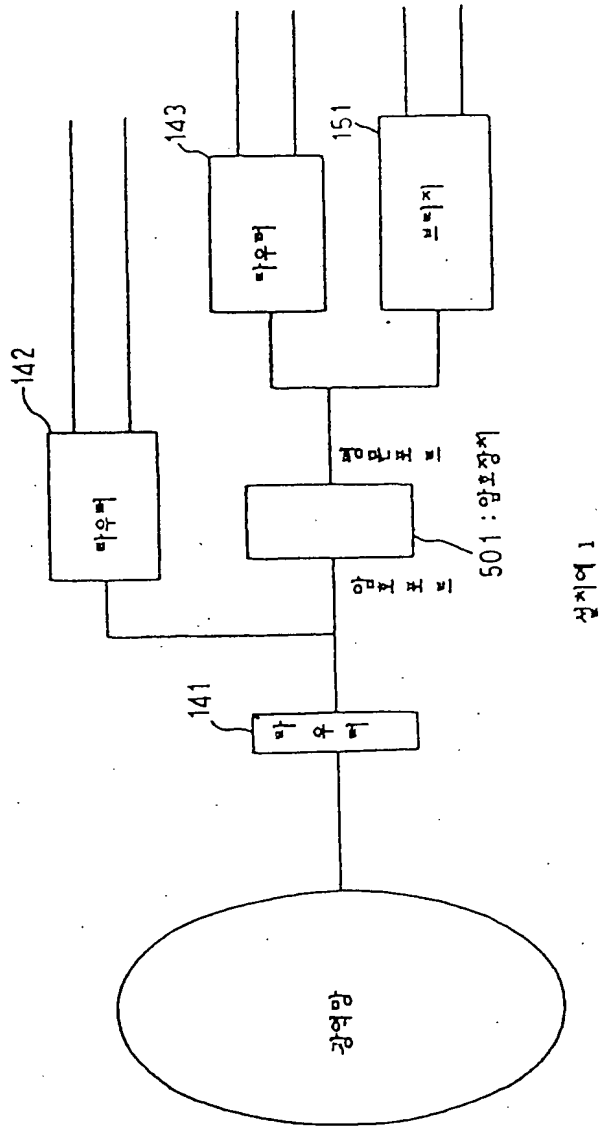
【도 28】



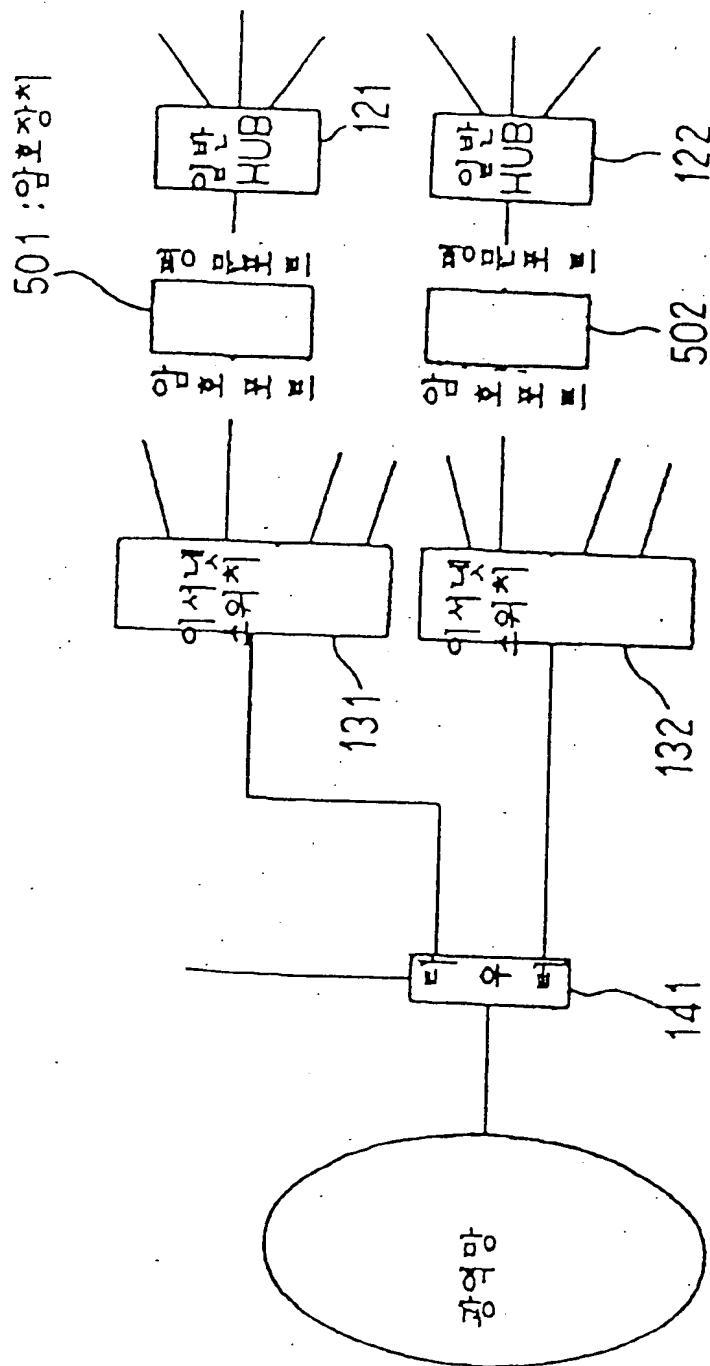
【도 29】



【도 30】

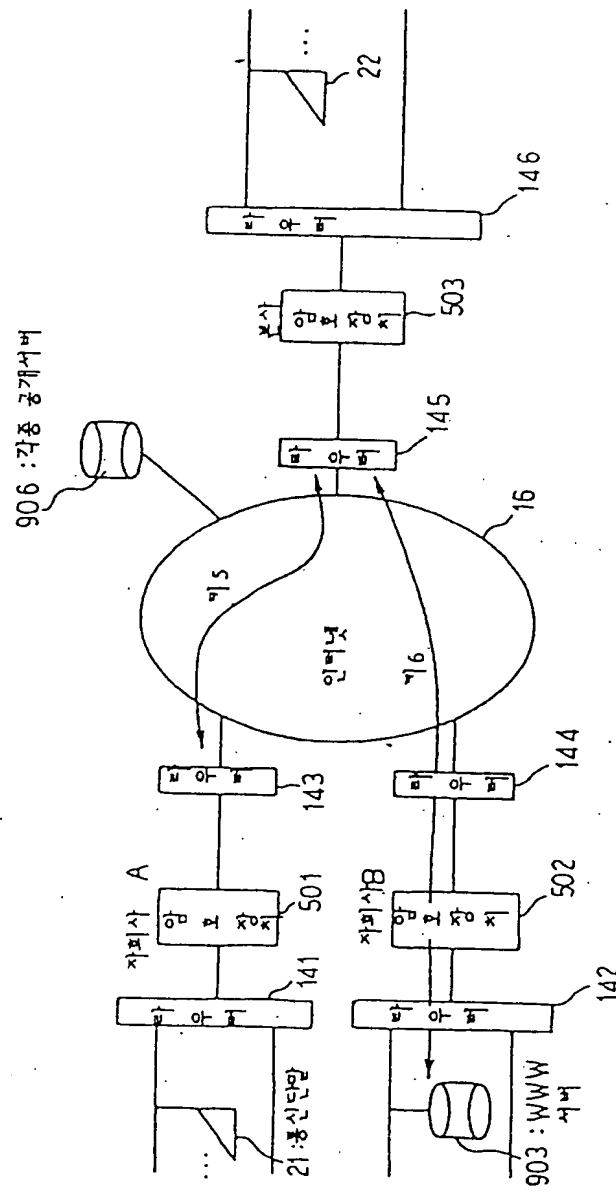


【도 31】

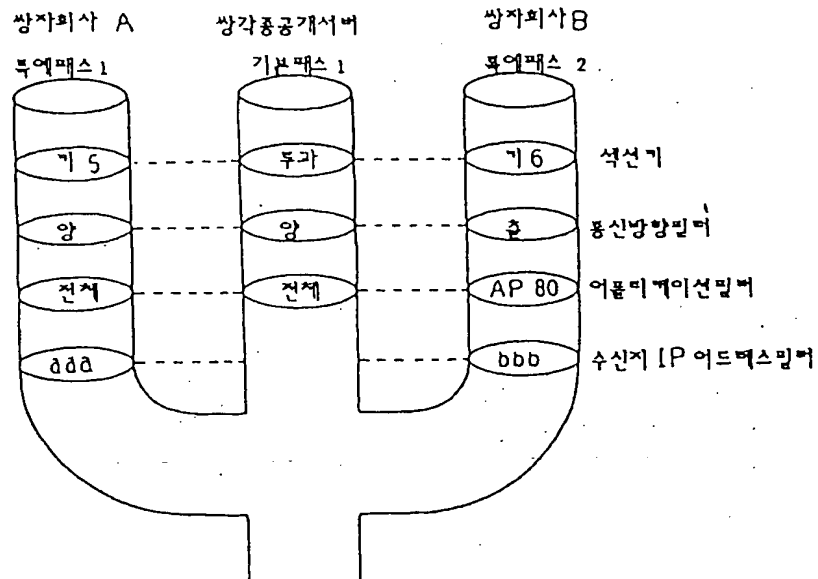


설치예 2

【도 32】



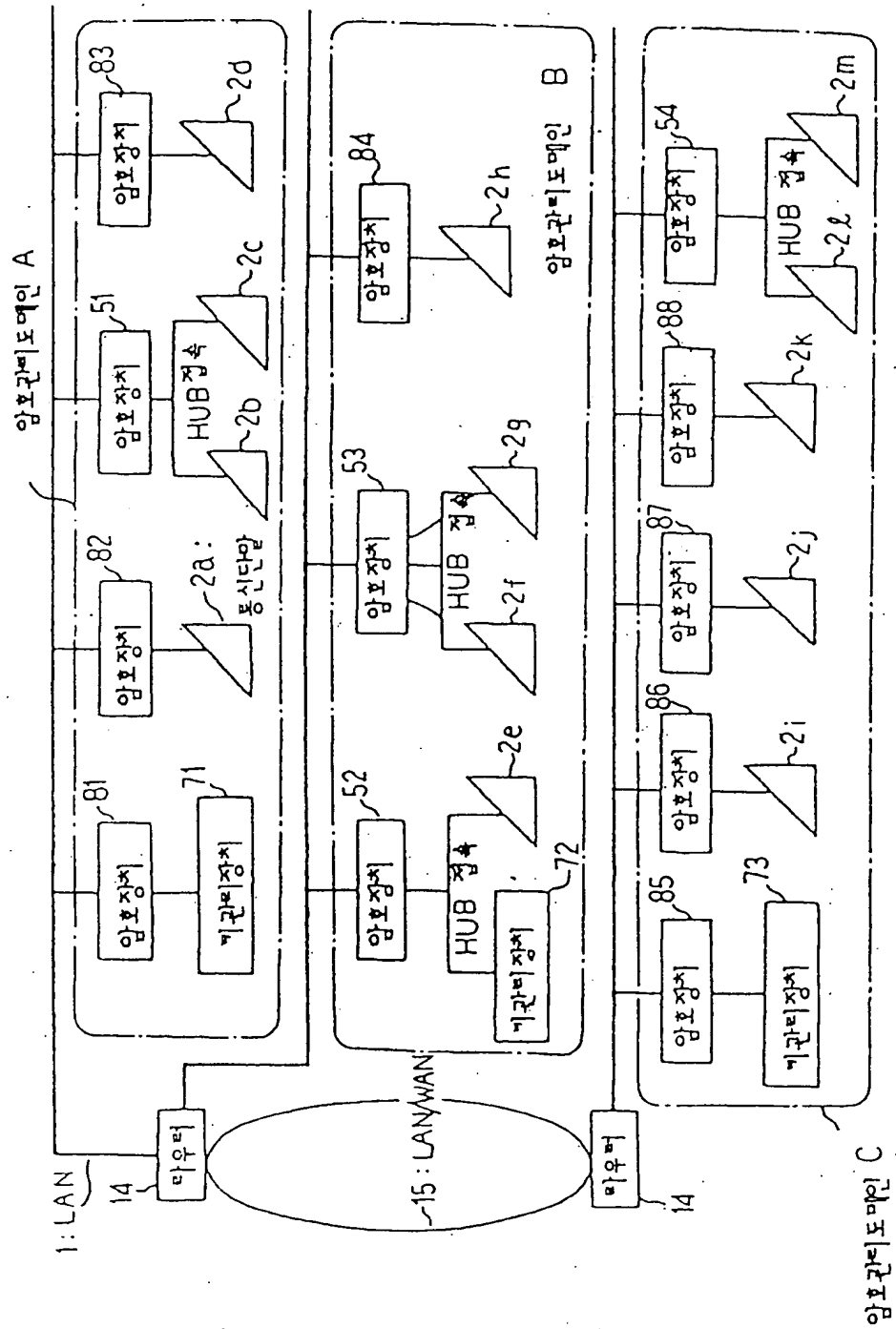
【도 33】



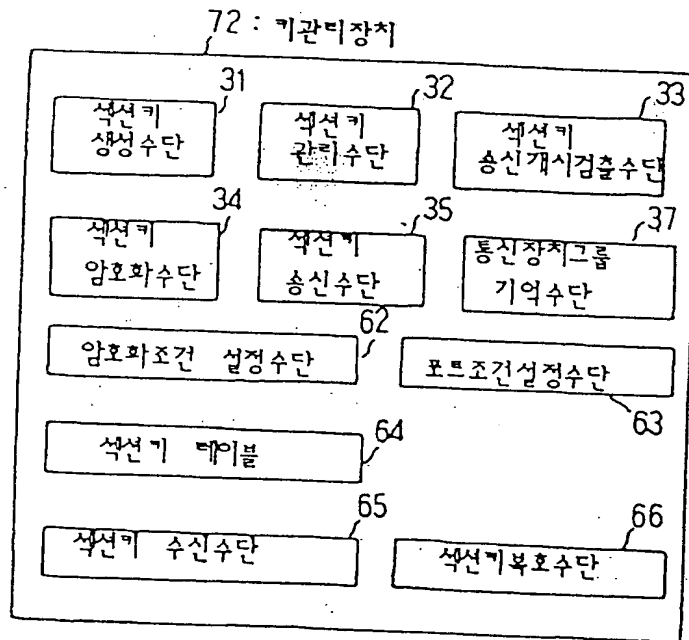
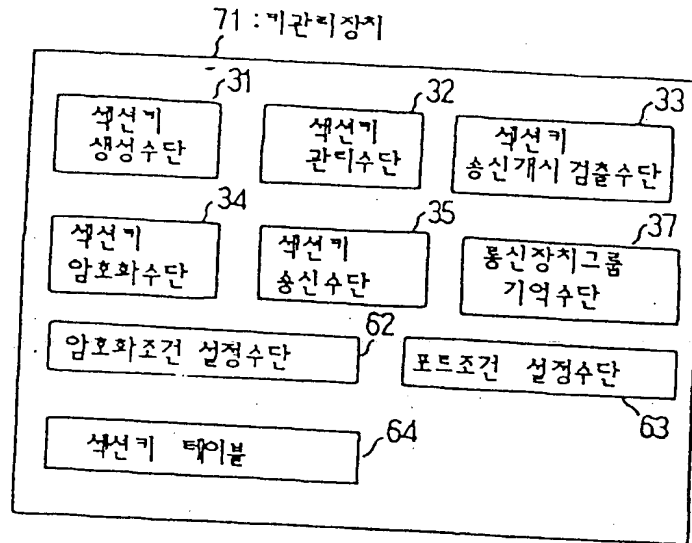
【도 36】

키번호	머가 플러그	키	속성
1	0	도널키 1	
2	0	도널키 2	
3	0	도널키 3	
4	0	도널키 4	
5	X	공통기 1	공통(A,B)
⋮	⋮		
8	X	공통기 2	공통(A,B)
⋮	⋮		
30	0	도널키 28	
31	0	도널키 29	
32	X	공통기 3	공통(A,B)

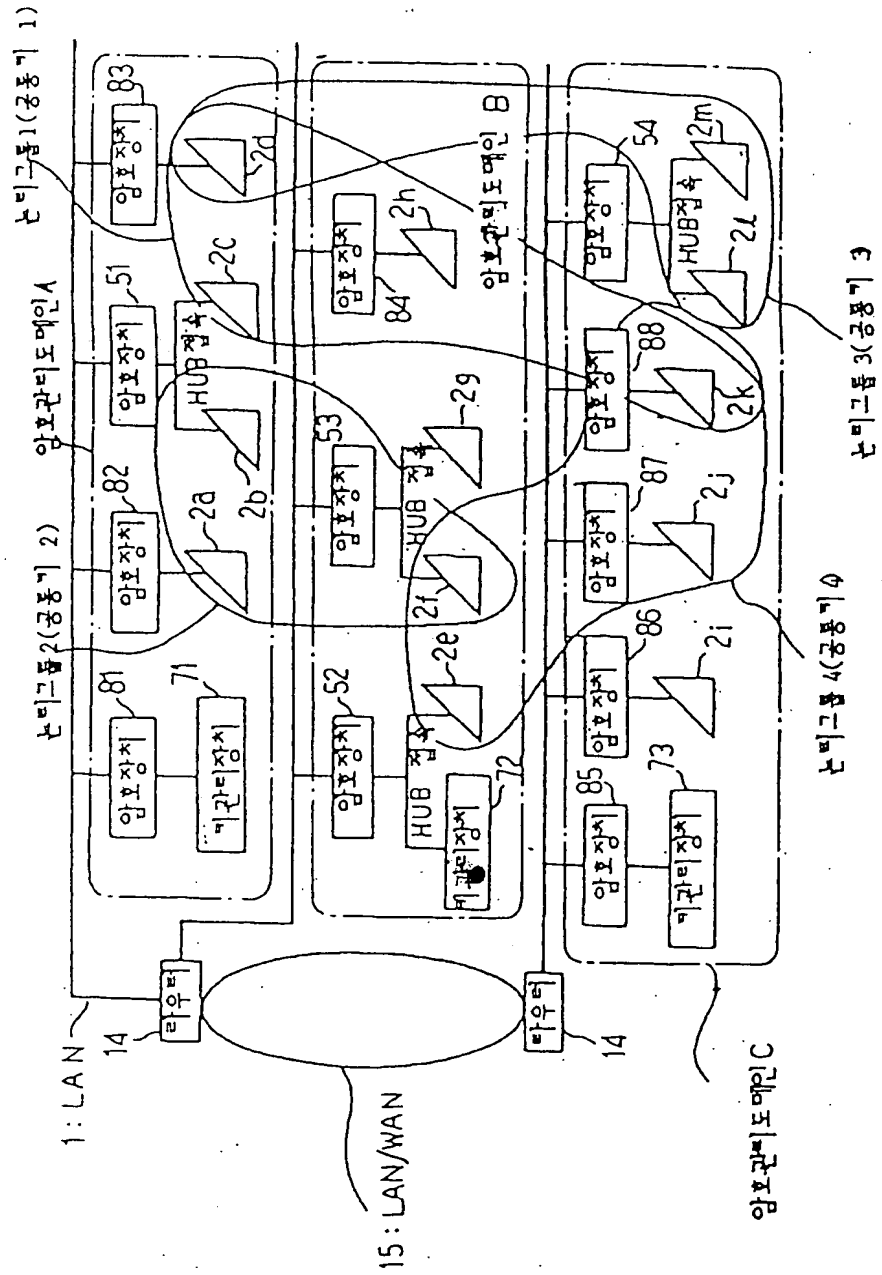
[도 34]



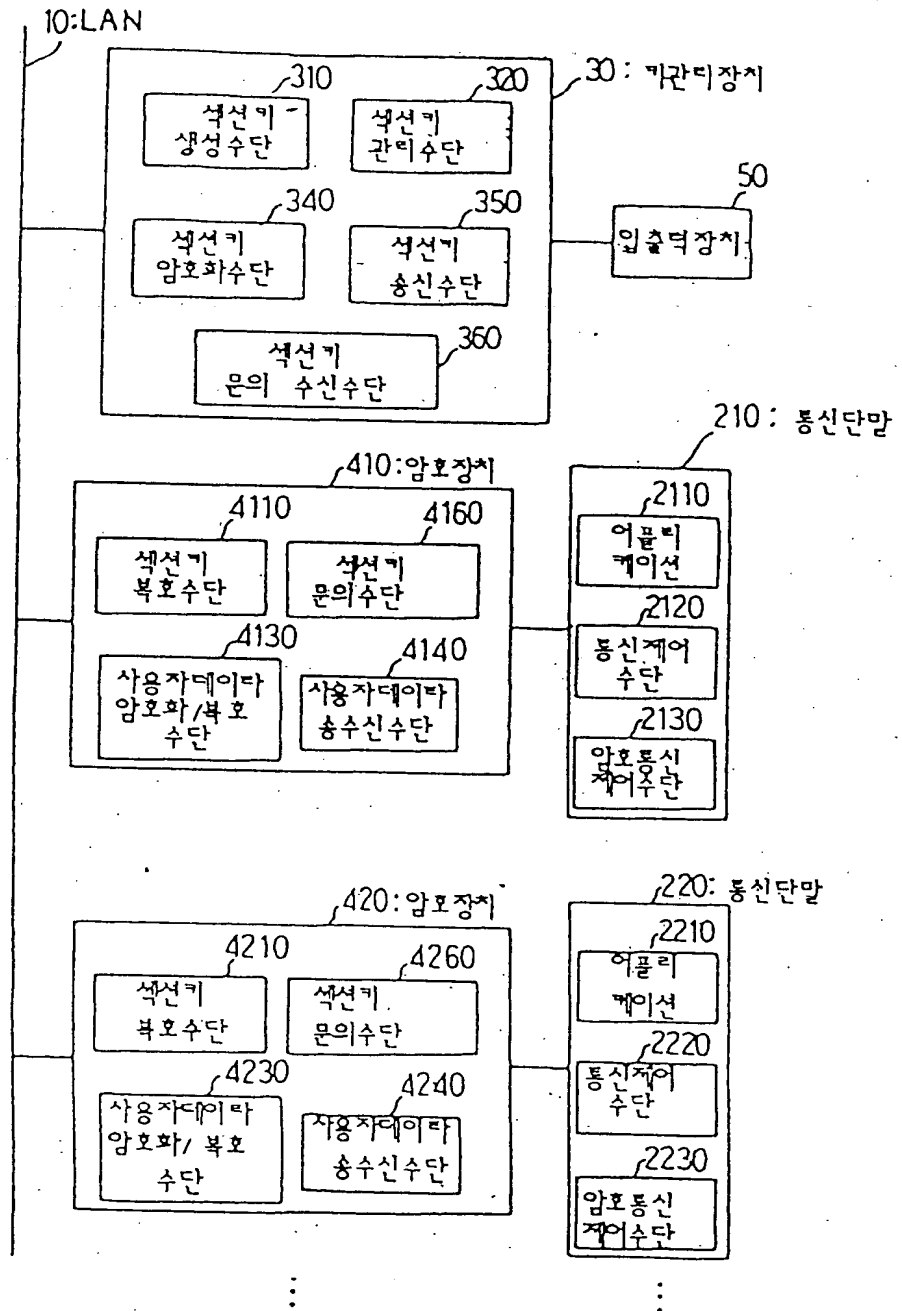
【도 35】



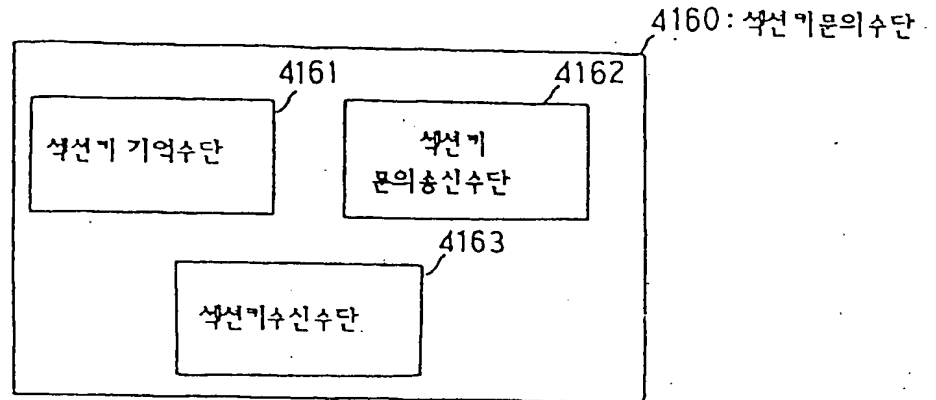
【도 37】



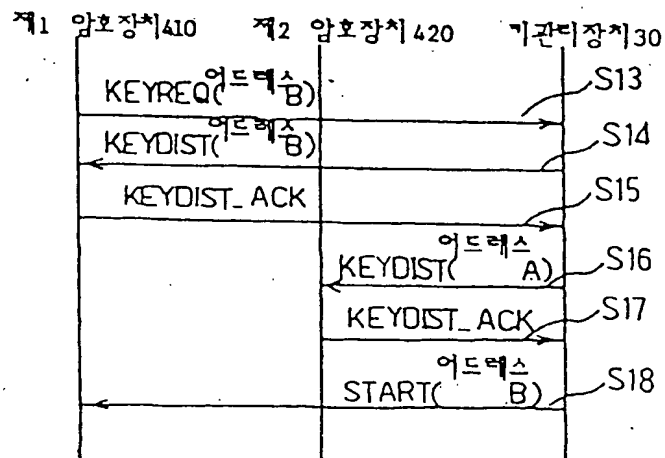
【도 38】



【도 39】



【도 40】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.